THE GREAT COURSES®

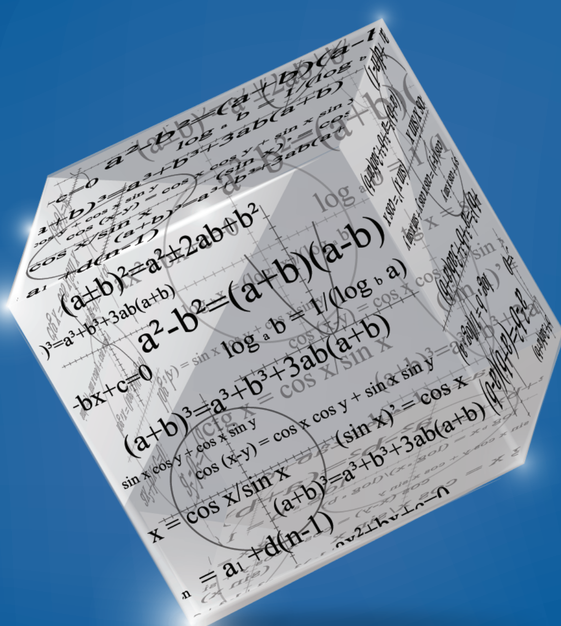
Topic
Science & Mathematics

Subtopic
Mathematics

Prove It: The Art of Mathematical Argument

Course Guidebook

Professor Bruce H. Edwards
University of Florida



PUBLISHED BY:

THE GREAT COURSES
Corporate Headquarters
4840 Westfields Boulevard, Suite 500
Chantilly, Virginia 20151-2299
Phone: 1-800-832-2412
Fax: 703-378-3819
www.thegreatcourses.com

Printed in the United States of America

Bruce H. Edwards, Ph.D.

Professor of Mathematics
University of Florida

Professor Bruce H. Edwards has been a Professor of Mathematics at the University of Florida since 1976. He received his B.S. in Mathematics from Stanford University in 1968 and his Ph.D. in Mathematics from Dartmouth College in 1976. From 1968 to 1972, he was a Peace Corps volunteer in Colombia, where he taught mathematics (in Spanish) at Universidad Pedagógica y Tecnológica de Colombia.

Professor Edwards's early research interests were in the broad area of pure mathematics called algebra. His dissertation in quadratic forms was titled "Induction Techniques and Periodicity in Clifford Algebras." Beginning in 1978, Professor Edwards became interested in applied mathematics while working summers for NASA at the Langley Research Center in Virginia. This led to his research in the area of numerical analysis and the solution of differential equations. During his sabbatical year, 1984 to 1985, he worked on 2-point boundary value problems with Professor Leo Xanthis at the Polytechnic of Central London. Professor Edwards's current research is focused on the algorithm called CORDIC that is used in computers and graphing calculators for calculating function values.

Professor Edwards has coauthored a wide range of mathematics textbooks with Professor Ron Larson of Penn State Erie, The Behrend College. Together, they have published leading texts in the areas of calculus, applied calculus, linear algebra, finite mathematics, algebra, trigonometry, and precalculus.

Over the years, Professor Edwards has received many teaching awards at the University of Florida. He was named Teacher of the Year in the College of Liberal Arts and Sciences in 1979, 1981, and 1990. He was both the College of Liberal Arts and Sciences Student Council Teacher of the Year and the

University of Florida Honors Program Teacher of the Year in 1990. He also served as the Distinguished Alumni Professor for the UF Alumni Association from 1991 to 1993. The winners of this 2-year award are selected by graduates of the university. The Florida Section of the Mathematical Association of America awarded Professor Edwards the Distinguished Service Award in 1995 for his work in mathematics education for the state of Florida. Finally, his textbooks have been honored with various awards from the Text and Academic Authors Association.

Professor Edwards has taught a wide range of mathematics courses at the University of Florida, from first-year calculus to graduate-level classes in algebra and numerical analysis. He particularly enjoys teaching calculus to freshman because of the beauty of the subject and the enthusiasm of the students.

Professor Edwards has been a frequent speaker at both research conferences and meetings of the National Council of Teachers of Mathematics. He has spoken on issues relating to the Advanced Placement calculus examination, especially on the use of graphing calculators.

Professor Edwards has taught 2 other Great Courses, *Understanding Calculus: Problems, Solutions, and Tips* and *Mathematics Describing the Real World: Precalculus and Trigonometry.* ■

Table of Contents

INTRODUCTION

LECTURE GUIDES

Table of Contents

Table of Contents

Prove It: The Art of Mathematical Argument

Scope:

The power and creativity of the human mind is nowhere more evident than in a clever, well-crafted argument. The most powerful and creative arguments, in turn, are to be found in mathematics, where the notion of proof is fundamental. For most people, however, the first—and frequently only—experience with mathematical proof comes in high school geometry, a time when students typically lack the maturity to appreciate the true beauty of proof. In this course, you will be presented with beautiful and important proofs from all areas of mathematics, many of which have become world famous for their elegance and creativity.

This course presumes no prior knowledge and will begin with the basics of logic and some foundational mathematical ideas. Armed with this background, you will proceed into the world of proof, discussing fundamental structure and various proof techniques—including direct proof, indirect proof, and proof by induction. As this course will emphasize throughout, appreciating the art of proof is one of the most enriching experiences that one can have.

The goal of this series of lectures is to appreciate the beauty and creativity of mathematical arguments. You will see theorems and proofs from a wide range of mathematical topics, including geometry, set theory, and number theory.

You will begin your study of proofs with an introductory lecture on the general nature of theorems and proofs. You will be presented with some examples of theorems that will be proven in subsequent lectures.

The second lecture briefly addresses Euclidean geometry. Euclid was perhaps the first mathematician to realize the importance of proof. His 13-book treatise, *Elements*, shows his understanding of the need to establish a list of definitions and axioms before proving theorems.

Because mathematical proofs rely on precise statements and logic, 3 lectures are devoted to elementary logic, including truth tables and quantifiers. Equipped with these tools, you will begin your study of elementary proof techniques, such as direct proofs and proofs by contradiction. You will encounter a classic indirect proof about the square root of 2.

Because set theory is used throughout mathematics, 2 lectures are devoted to proofs in this field. In particular, you will examine the surprising properties of infinite sets. You will discover that defining the "size" of an infinite set requires some precise language. In fact, you will see that one set can be contained in another—yet they have the same "size."

Mathematical induction is one of the most powerful weapons that mathematicians possess for proving theorems involving the counting numbers, so 3 lectures will be devoted to this proof technique. In this section of the course, you will prove results on summations, division properties, and even the famous Fibonacci numbers.

Many theorems in mathematics involve the existence of a certain mathematical object, and other theorems establish the uniqueness of a mathematical object. Hence, 2 lectures will be dedicated to these existence and uniqueness questions. You will also study a proof technique in which the validity of a statement is established by analyzing all the possible cases.

One can learn a lot about reading and writing proofs by looking at conjectures, or statements, that are in fact false. Hence, you will study the role of counterexamples in mathematics. In addition, a lecture will be devoted to false proofs, in which the mathematical arguments seem plausible but are actually incorrect.

It is said that a picture is worth a thousand words, and this is also true in mathematics. You will be presented with some wonderful visual explanations of mathematics theorems, including the famous Pythagorean theorem.

Number theory is one of the oldest areas of mathematics and contains many beautiful theorems and proofs. You will study the prime numbers, including their distribution and properties. The lectures on number theory will also present some famous unsolved problems, including Goldbach's conjecture and the twin prime conjecture. These unsolved problems are easy to understand, but their proofs have eluded mathematicians to this day.

At the end of this series of lectures, you will examine 2 slightly more advanced topics: the theory of perfect numbers and the famous number e. You will use a variety of proof techniques to study the properties of perfect numbers, including a theorem attributed to Euclid. In the final lecture, you will use techniques from infinite series to prove that the number e, the base of the natural logarithm, is in fact an irrational number. ■

What Are Proofs, and How Do I Do Them?

Lecture 1

Early mathematical training often focuses on memorization and computation instead of on formal arguments and proofs. However, upper-level math courses—postcalculus courses at universities, such as analysis, linear algebra, and topology—have a very solid foundation in proofs and emphasize precise mathematical reasoning. One of the goals of this course is to explain what a mathematical proof is and to show you what kinds of mathematical proofs exist. In addition, this course will show you the beauty and creativity of proofs. You'll be exposed to many proofs as the course progresses, but you'll also learn how to write your own proofs. Perhaps most importantly, this course will hopefully motivate you to explore many of the themes and topics that are addressed in more detail.

Numbers and Number Systems

- Integers are the numbers 0, 1, 2, 3, 4, and so on and the negative numbers −1, −2, −3, −4, and so on. For example, −12 is an integer and 9 is an integer, but 1/2 and 2/3 are not integers. Pi, the famous number that is approximately equal to 3.14159, is not an integer either.

- Integers are divided up into 2 groups or sets: the odds and the evens. The even integers are 0, 2, 4, 6, 8, and so on and also −2, −4, −6, −8, and so on. An even integer is 2 times another integer. For example, 8 is even, and it is equal to 2×4. In addition, $10 = 2 \times 5$, $0 = 2 \times 0$, and $-6 = 2 \times -3$.

- An integer n is even if it is of the form $n = 2k$, where k is an integer.

- The odd integers are 1, 3, 5, 7, and so on and also −1, −3, −5, −7, and so on. An odd number, or odd integer, is an even number plus 1. For example, $7 = 6 + 1$, or an even number plus 1.

- An integer n is odd if it is of the form $n = 2k + 1$, where k is an integer.

- The integer 7 is an odd integer because it is equal to $2 \times 3 + 1$, or $2k + 1$. The integer -9 is odd because it is equal to $2 \times -5 + 1$, or $-10 + 1$.

- We defined the odd integers of the form $2k + 1$, but we could also use $2k - 1$. These are equivalent definitions; both work perfectly well as definitions of odd numbers.

Examples of Proofs

- What is an even integer times an even integer? For example, $4 \times 6 = 24$; 4 is even, 6 is even, and the product (24) is even. In addition, $8 \times -2 = -16$. An even integer times an even integer seems to always yield an even integer.

- To prove that the product of 2 even integers is always an even integer, let's begin with 2 even integers, which means that each one is 2 times another integer. Let's call the 2 even integers $2k$ and $2s$. The product of these 2 even integers, $2k \times 2s$, will be even if it is 2 times an integer. The product $2k \times 2s$ is equivalent to $4ks$ ($2 \times 2 = 4$), and if we factor out a 2, then the product is $2(2ks)$. The product of those 2 even integers is 2 times an integer ($2ks$), making it even by definition.

- To prove that an odd integer times an odd integer yields an odd integer, consider 2 odd integers $2n + 1$ and $2k + 1$. Using some algebra, start by multiplying the 2 odd integers: $(2n + 1) \times (2k + 1) = 4nk + 2n + 2k + 1$. To determine if that product is odd, factor a 2 out of the first 3 terms to get $2(2nk + n + k) + 1$. That result is odd because it is 2 times an integer $(2nk + n + k)$ plus 1. This proof is called a direct proof because you started with 2 odd integers and directly did some algebra and math to arrive at the conclusion.

Proofs, Theorems, and Conjectures

- There are other number systems besides the integers. The rational numbers are the fractions, or the quotients of integers a/b, where b cannot be 0 (because you can't divide by 0 in mathematics). For example, 1/2 is a rational number, and it's not an integer. However, 3 is an integer, but it's also a rational number: It's a fraction because 3 is the same as the quotient 3/1. In addition, 0 is a fraction; it is 0/1. It is a rational number.

- A proof is a logical argument that establishes the truth of a statement or theorem. The best proofs in mathematics hopefully are short and elegant, and they hopefully provide some insight into why the theorem is true. One of the tools in proving theorems in mathematics is using logic, which will be used throughout these lectures.

- Proofs in mathematics are really quite different from proofs in other disciplines. For example, in biology, a proof might consist of experimental data confirming some conjecture, and in psychology, a proof might consist of survey results. On the other hand, math is extremely rigorous. The arguments aren't based on data; instead, they are solidly based on logic and other theorems. The best proofs—the most rigorous proofs—are mathematical proofs.

- A theorem is a statement in mathematics that has been proven. For example, the Pythagorean theorem is a theorem about right triangles that says that if you have a right triangle and the 2 short sides (or legs) measure x and y and the hypotenuse measures z, then $x^2 + y^2 = z^2$. An example of a right triangle that satisfies the Pythagorean theorem is the 3-4-5 right triangle, in which the legs measure 3 and 4 and the hypotenuse measures 5: $3^2 + 4^2 = 5^2$, or $9 + 16 = 25$. There are many proofs of the Pythagorean theorem.

- A theorem that is closely related to the Pythagorean theorem is Fermat's last theorem. In the Pythagorean theorem, $x^2 + y^2 = z^2$, the exponents are 2, 2, and 2. Suppose that you changed the exponents to 3, 3, and 3 ($x^3 + y^3 = z^3$) or 4, 4, and 4 ($x^4 + y^4 = z^4$). That's Fermat's last theorem—a very famous theorem in mathematics. Fermat claimed that for each integer n greater than or equal to 3, there are no positive integer solutions x, y, and z such that $x^n + y^n = z^n$. In other words, there are many solutions when $n = 2$ but no solutions when $n = 3$ or higher. This theorem has an amazingly long history and was very recently proven in a very difficult proof.

- Some conjectures, or statements, remain unproven. It's not even clear if they are true or false; they are unsolved problems. An example of this is the Collatz conjecture, which is sometimes called the $3n + 1$ conjecture. To start, choose a positive integer. If that number is even, divide it by 2. If it's odd, multiply it by 3 and add 1.

- For example, your positive integer is 6. It's even, so you divide it by 2 and are left with 3, which is odd. The rule says to multiply it by 3 and add 1: $3 \times 3 = 9$, and $9 + 1 = 10$. Because 10 is even, you then divide it by 2 and are left with 5. Because 5 is odd, you then multiply it by 3 and add 1: $5 \times 3 = 15$, and $15 + 1 = 16$. Because 16 is even, you then divide it by 2, which gives you 8. Because 8 is even, you divide it by 2, which gives you 4. Because 4 is even, you divide it by 2, which gives you 2. Because 2 is even, you divide it by 2, which is 1.

- Collatz observed that these sequences of numbers always terminate at 1—but nobody has been able to prove that this result is always true. Nobody knows if there exists a gigantic number that never terminates at 1, and there have been many computer studies that have been conducted that can't prove it either.

Problems

1. Prove that the sum of an even number and an odd number is odd.

2. How does a proof in mathematics differ from proofs in other disciplines?

The Root of Proof—A Brief Look at Geometry

Lecture 2

Euclidian geometry, as developed in *Elements* by Euclid, is the model of all mathematical thinking today. Euclid began with definitions, axioms, and common notions and then proved propositions, or theorems. He recognized the crucial fact that not everything can be proven. Similarly, modern mathematicians start with some undefined terms and axioms and then prove theorems using logic. In this lecture, you will learn about some of the theorems in Euclid's work, and you will discover that geometry is the root of proof.

Euclid's *Elements*

- Early mathematics was involved with calculations, such as finding the area of a field or the volume of a container. The Greeks were the first people in the Western hemisphere to start to do real proofs. They wanted to know the reasoning behind certain propositions or theorems. The most important work dealing with proofs is Euclid's *Elements*—developed around the third century B.C.—which basically consists of 2 parts: geometric theorems and number theory.

- In producing *Elements*, which consists of 13 books on geometry and number theory in total, Euclid realized that you can't prove everything. You have to have a set of axioms or postulates, and from those, you begin to prove your theorems. In fact, all pure mathematics today is based on the idea of an axiomatic system. After you've established that axiomatic system and accept those axioms, then the theorems can be developed—one after the other.

- Euclid began his treatment of geometry with certain definitions: For example, a point is that which has no part, a line is breadthless length, and an obtuse angle is an angle greater than a right angle. In a sense, these aren't great definitions.

- Modern mathematicians realize that you can't define everything because the arguments and definitions become too circular. Instead, they begin with certain undefined terms, and from there, they develop axioms and theorems. In general, to prove theorems, you start with a certain proposition and then arrive at a conclusion.

- Euclid's famous 5 postulates are as follows.
    - Given 2 points, you can draw a line between them. In other words, 2 points determine a line.
    - A straight line can be extended in both directions indefinitely.
    - Given a line segment, a circle can be drawn with one of the endpoints as the center and the segment as the radius.
    - All right angles are equal to each other.
    - The fifth postulate is much more complicated than the first 4, but an equivalent statement of this postulate is: Given a point not on a line, there exists 1 and only 1 line through that point parallel to the given line.

- In *Elements*, Euclid also laid down some common notions, which are really everyday algebraic properties that we all accept.
    - Things that equal the same thing are also equal to one another. In modern language, this notion is similar to the following: If $a = b$ and $a = c$, then $b = c$.
    - If equals are added to equals, then the wholes are equal.
    - The whole is greater than the part.

- Euclid clearly recognized that you can't prove everything. Postulates and common notions are the starting points, and then the theorems follow. Euclid's work, *Elements*, is the foundation of how we do mathematics today. Euclid set the standard for proofs and logical arguments.

Euclid's Early Theorems

- Euclid's proposition 1, his first theorem, states (in modern notation) that from a given line segment—using a straight edge and compass only—you can construct an equilateral triangle, which is a triangle that has 3 equal sides.

- For example, on line segment AB (drawn between the 2 points A and B), using a compass, you can draw a circle with its center at A and with radius AB. Then, you can draw another circle with its center at B and the same radius AB. Those 2 circles intersect at a point that you can label as C. Then, you can draw the segment AC and the segment BC, which—together with segment AB—result in an equilateral triangle. AB, AC, and BC are all equal in length because a compass was used to preserve those lengths.

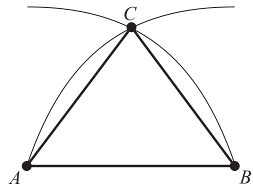


Figure 2.1

- Euclid's proposition 5 has to do with isosceles triangles. You're given a triangle ABC, and you assume that AB and AC have equal length, or are congruent legs of the triangle. You're supposed to prove that the angle at B is congruent to the angle at C. Basically, you are given a triangle that has 2 equal sides and you have to prove that it has 2 equal angles—that the 2 base angles are congruent to each other.

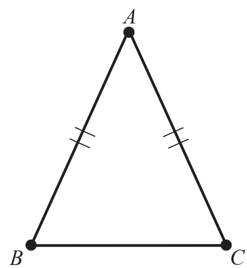


Figure 2.2

- A simpler proof can be found in most high school and college geometry textbooks. You're given a triangle ABC. Bisect the angle at A, producing 2 triangles. That angle bisector intersects the side BC at the point D. One of the 2 triangles that is produced is BAD, and the other is CAD. These triangles are congruent to each other because BA is congruent to CA, the angle at A has been bisected into 2 congruent angles at A, and the segment AD is congruent to itself. Therefore, the 2 triangles are congruent by the side-angle-side formula. The triangles are congruent, and corresponding parts of congruent triangles are congruent. In particular, the angle at B is congruent to the angle at C.

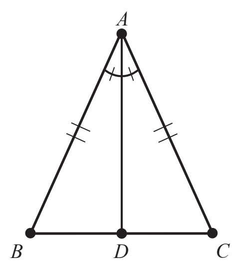


Figure 2.3

- The next proof requires you to look at the triangle BAC from a different perspective; in other words, flip it over and consider it as another triangle CAB. You will find that the triangle is congruent to itself if you flip it over. Segment BA is congruent to segment CA, included angle A is congruent to itself, and segment AC is congruent to segment AB. Therefore, triangle ABC is congruent to triangle ACB by the side-angle-side formula. Hence, the corresponding parts are congruent. For example, the angle at B is congruent to the angle at C.

- *Elements* is, of course, not perfect. There are some problems with Euclid's definitions, and there are some other gaps in his work. Fortunately, later mathematicians developed a better set of undefined terms, definitions, and axioms. Today, geometry is on solid ground, even though everyone does not agree on the set of axioms.

- All Euclidian geometry textbooks start with a set of axioms and some undefined terms and, from there, prove theorems. As progress is made—after theorem 1, theorem 2, and theorem 3 have been proven—those theorems can be used to prove the next theorem. More and more complicated theorems are arrived at as the string of propositions and theorems is built.

Euclid's Fifth Postulate

- Historically, mathematicians didn't think that Euclid's fifth postulate was really a postulate or an axiom; instead, they thought it should be a theorem. In other words, they thought that the fifth postulate should be able to be derived as a theorem from Euclid's axioms, definitions, and common notions.

- Over a span of 2000 years of attempts to prove the fifth postulate from the rest of Euclid's postulates, there are many sad stories of mathematicians dedicating their lives to the idea of proving it without success. Finally, 3 mathematicians independently—in different parts of the world—showed that Euclid's parallel postulate could not be proven from the other postulates. These 3 mathematicians were the Hungarian mathematician János Bolyai, the Russian mathematician Nikolay Lobachevsky, and the German mathematician Carl Gauss.

- These 3 mathematicians showed that you could alter Euclid's fifth postulate and obtain a new geometry equally as valid as Euclidian geometry. In other words, not only was the fifth postulate not provable from Euclid's axioms, but you could also change the postulate and construct a brand new geometry that is equally as valid as Euclidian geometry.

- The new postulate is as follows: Given a line and a point off the line, there are at least 2 lines through the point p that are parallel to the line m. In fact, there are an infinite number of parallels to the line because any line in between the 2 lines that you draw will be parallel as well.

- This geometry—often called non-Euclidian geometry—is equally as consistent as Euclidian geometry in the following sense: If there's a contradiction or flaw in this new geometry, then there's a corresponding flaw in Euclidian geometry. If one is correct, then so is the other, and if one is incorrect, then so is the other.

PROBLEMS

1. If $AB = AC$ in ΔABC, then $\angle ABC \cong \angle ACB$. Prove this by bisecting the angle at A, intersecting the segment $\overline{BC}$ at D.

2. Use angle-side-angle to prove that if a triangle has 2 congruent angles, then the triangle is isosceles.

The Building Blocks—Introduction to Logic

Lecture 3

This is the first of 3 lectures on logic, which serves as the foundation of how mathematicians prove theorems. In this lecture, you will learn about such connecting words as "and" and "or" in dealing with statements and propositions. You will also learn that statements can be either true or false—but not both. Given 2 statements, you will combine them as conjunctions and disjunctions. In addition, you will construct truth tables, which are very useful in analyzing compound statements.

More Number Systems

- Recall that the integers are 0, 1, 2, 3, 4, and so on and then −1, −2, −3, −4, and so on. The positive integers—1, 2, 3, 4, and so on—are often called the natural numbers.

- After the integers, there is a bigger set of numbers called the rational numbers. These are the fractions, or the quotients *a*/*b* of integers. Examples of rational numbers include 3/2 and 7/9.

- Some numbers are not rational numbers; they are called irrational numbers. In fact, the set of all real numbers is split into 2 groups: rational numbers and irrational numbers.

- Complex numbers are numbers that include $\sqrt{-1}$, for example. Complex numbers will not be used very much in these lectures, but you might have heard of them.

Mathematical Statements

- A statement can be either true or false—but not both. In mathematics, the statement that 7 is a natural number is true. However, the statement that −4 is a natural number is false.

- Suppose that P is the statement "It is Tuesday" and that Q is the statement "I am swimming." Then, the combination is P and Q, which would be the mathematical statement "It is Tuesday and I am swimming." This statement would be true if both pieces are true—in other words, if it's true that it's Tuesday and if it's true that I am swimming. Otherwise, it would be a false statement.

- This usage of "and" in mathematics is not the same as its everyday usage in English. For example, in math, "P and Q" is the same as "Q and P." The order is not important. However, this is not true in everyday usage. Consider the following phrase: "Bruce kicked the ball and the field goal was good" is not the same as "The field goal was good and Bruce kicked the ball."

- The word "and" is often called a conjunction between the 2 statements P and Q, and its symbol is a wedge pointing upward ($\wedge$). It's often called the "meet" of the statements P and Q, or the wedge.

- What does P or Q mean? The statement would be "It is Tuesday or I am swimming." In mathematics, this statement is true if it is Tuesday or if I am swimming. Furthermore, if it is Tuesday and I am swimming, it would also be true. The only time it's false is when both pieces are false.

- The word "or" is often called a disjunction, and it's independent of order. P or Q is the same as Q or P. The notation is similar to the notation for "and." It's the wedge turned upside down ($\vee$), and it's often called the "join" of P and Q.

- The mathematical usage of the word "or" is not the same as its everyday usage in English. Math uses the inclusive or. When you write the statement P or Q, that's true if P is true or if Q is true—or if both are true. With the exclusive or, which is the everyday English usage of the word, you don't have both the quality that both are true. For example, the door is open or closed. It's either open or closed, but it can't be both.

- In mathematics, $a < b < c$ means that a is less than b and b is less than c. It's an "and" statement. However, $a \le b$ means that a is less than b or a equals b. It's an "or" statement.

- For example, $2 < 4 < 7$ means that 2 is less than 4 and 4 is less than 7. Furthermore, $5 \le 8$ is a true statement, and $5 \le 5$ is also a true statement because 5 equals 5. However, $2 \le 1 < 5$ is a false statement. Of course, 1 is less than 5 and 2 is less than 5, but 2 is not less than or equal to 1. In addition, $4 > 4$ is false because $4 = 4$.

- Suppose that you had a product of 2 numbers equal to 0. A theorem says that $a = 0$ or $b = 0$, which is an "or" statement. The conclusion is that a is 0 or b is 0, and in fact, they both could be 0. The fact that the product equals 0 implies that one or both of the 2 terms is 0.

Truth Tables

- One way to analyze statements that involve "and" and "or" is by building truth tables. For example, if you combine 2 statements into the statement "*P* and *Q*," there are 2 possibilities for *P* (true or false), and there are 2 possibilities for *Q* (true or false). Together, there are 4 possible combinations: both are true (TT), both are false (FF), the first one is true and the second one is false (TF), or the first one is false and the second one is true (FT).

- If you put these together in a table, in the first column, you have the possible *P* values: true, true, false, false. In the second column, you have the possible *Q* values: true, false, true, false. If you look at the first 2 columns together, you see the 4 possible cases. In the third column, you write down the truth values for the conjunction *P* and *Q*.

- *P* and *Q* is true if both statements are true, so the first entry in the third column is true. Then, the other 3 entries are false. The entry in the second row in the third column is false because *Q* is false. In the third row, it's false because *P* is false. In the fourth row, it's false because both *P* and *Q* are false. (See Table 3.1.)

- Alternatively, the truth table for "or" would have the exact same first 2 columns as the previous "and" truth table, but the third column is different. Because "or" is true if either entry is true or if both entries are true, the third column is true, true, true, false. The only time it's false is when both P and Q are both false. (See Table 3.1.)

Table 3.1

P	Q	P and Q	P or Q
T	T	**T**	**T**
T	F	**F**	**T**
F	T	**F**	**T**
F	F	**F**	**F**

- For the compound statement $(P \vee Q) \wedge R$, there are 2 possibilities for P, 2 for Q, and 2 for R, which results in 8 rows in the truth table. In the first column are the truth values for P, and the first 4 are all true while the next 4 are all false. The second column consists of the Q values, which are true, true, false, false, true, true, false, false. Finally, the values for R are true, false, true, false, true, false, true, false.

- Let P be the statement "I like red wine." Let Q be the statement "I like dark chocolate." Let R be the statement "I am 65 years old." The statement $(P \vee Q) \wedge R$, then, would be a combination of those 3 statements: I like red wine or I like dark chocolate, and I am 65 years old.

- To calculate the values in the fourth column, you have to form $P \vee Q$, which is an "or" statement, so it will be true except if both statements in the first 2 columns are false. In rows 7 and 8, both entries for P and Q are false, so in the fourth column, rows 7 and 8 are false, but all the others—the first 6 entries—are true.

- To determine the final answer, $(P \vee Q) \wedge R$, you have to look at the third column, R, and the fourth column, $P \vee Q$. Because this final statement is an "and" statement, there is only a true value if both entries are true. In particular, it's true in the first row, third row, and fifth row. There are 3 places where this statement is true and 5 where it is false. (See Table 3.2.)

Table 3.2

P	*Q*	*R*	*P* or *Q*	(*P* or *Q*) and *R*
T	T	T	T	**T**
T	T	F	T	**F**
T	F	T	T	**T**
T	F	F	T	**F**
F	T	T	T	**T**
F	T	F	T	**F**
F	F	T	F	**F**
F	F	F	F	**F**

- The previous compound statement, $(P \vee Q) \wedge R$, is actually equivalent to the compound statement $(P \wedge R) \vee (Q \wedge R)$, which is an "or" statement with these 2 phrases. You could show that the previous statement is equivalent to the new statement by constructing the truth table for the new statement and comparing it to the previous table.

Table 3.3

P	*Q*	*R*	*P* and *R*	*Q* and *R*	(*P* and *R*) or (*Q* and *R*)
T	T	T	T	T	**T**
T	T	F	F	F	**F**
T	F	T	T	F	**T**
T	F	F	F	F	**F**
F	T	T	F	T	**T**
F	T	F	F	F	**F**
F	F	T	F	F	**F**
F	F	F	F	F	**F**

- In another example, the statement P is "−7 is a natural number." That statement is false because −7 is not a natural number. (It's a negative integer.) The statement Q is "4/5 is a rational number."

That is true; it's a fraction. The third statement is "pi is a positive, real number." That is true. Pi is equal to about 3.14159, and it's a positive, real number.

- $P \wedge Q$ is false because P is false and it's an "and" statement. $P \vee Q$ is true because the Q part is true. $P \wedge R$ is false because P is false. $P \vee R$ is true because R is true. $Q \wedge R$ is true because both Q and R are both true. $Q \vee R$ is also true because they are both true.

PROBLEMS

1. Describe in words the meaning of the mathematical statement $a \geq b > c$.

2. Construct the truth tables for $(P \wedge Q) \vee R$ and $(P \vee R) \wedge (Q \vee R)$. What do you observe?

More Blocks—Negations and Implications

Lecture 4

In the last lecture, you learned about the connectors "and" and "or," and in this lecture, you will continue your study of logic—the language of mathematics. In this lecture, you will learn about negations of statements. Then, you will learn about implications, or statements in which the hypothesis implies the conclusion (for example, "if P, then Q"). Most mathematical theorems are implications, but negations can be very interesting. In addition, you will learn about equivalent statements.

Negation

- Negation involves the interchanging of true and false in a logical statement. The negation of a statement is true if the statement itself is false. Conversely, the negation of a statement is false if the original statement is true.

- For example, the negation of the statement "The number 6 is even" is "The number 6 is odd." In this case, the original statement is true, and its negation is false. However, the negation of the statement "The number 8 is odd" is "The number 8 is not odd." Hence, the number 8 is even. In this case, the negation is the true statement.

- In textbooks, negation is often denoted by a horizontal line that has a little vertical tail on it: ¬. However, other textbooks use a little wiggle: ~. Be aware that these notations vary among books.

- What is the negation of the statement $a < b$? The negation of "a is less than b" is "a is not less than b," which is equivalent to $a \geq b$. Furthermore, the negation of $a = b$ is $a \neq b$. The negation of $a \neq b$ returns to the original statement $a = b$.

- What is the negation of $P \wedge Q$? Suppose that P is the statement "It is Tuesday" and Q is the statement "I am 65 years old." Therefore, $P \wedge Q$ would be the statement "It is Tuesday and I am 65 years old."

The negation of that is “It is not Tuesday or I am not 65 years old.” Notice that the “and” statement converted into an “or” statement.

- The theorem becomes $\neg(P \wedge Q) = (\neg P) \vee (\neg Q)$. To prove this theorem, construct the truth table for $\neg(P \wedge Q)$ and then the truth table for $(\neg P) \vee (\neg Q)$ and compare them. They should be the same.

- The first column consists of the P possibilities: true, true, false, false. The second column for Q is true, false, true, false. The first 2 columns always look the same. The third column for $P \wedge Q$ is true, false, false, false. $P \wedge Q$ is true only in the case where both P and Q are true. To build the fourth column, $\neg(P \wedge Q)$, you have to negate the third column. Therefore, every time you see a true in the third column, put a false in the fourth column. Conversely, every time you see a false, put a true. The results for the fourth column end up being false, true, true, true. (See Table 4.1.)

Table 4.1

P	***Q***	***P* and *Q***	**Not (*P* and *Q*)**
T	T	T	**F**
T	F	F	**T**
F	T	F	**T**
F	F	F	**T**

- Next, compare the previous truth table to the truth table for $(\neg P) \vee (\neg Q)$. The first and second columns are the same as before. Then, for the third column, which is $\neg P$, take the first column and change each one—from true to false and from false to true. Therefore, you are left with false, false, true, true. For the fourth column, which is $\neg Q$, reverse each entry in the second column, and you are left with false, true, false, true. Then, columns 3 and 4 need to be joined with “or,” which is true if either one is true or both are true. The second, third, and fourth rows are all true. The only time it’s false is in the first row, when both $\neg P$ and $\neg Q$ are false. The 2 truth tables are the same. (See Table 4.2.)

Table 4.2

P	***Q***	**Not *P***	**Not *Q***	**(Not *P*) or (Not *Q*)**
T	T	F	F	**F**
T	F	F	T	**T**
F	T	T	F	**T**
F	F	T	T	**T**

- The statement that was just proved using truth tables, $\neg(P \wedge Q) = (\neg P) \vee (\neg Q)$, is one of De Morgan's laws, which are named after a very famous mathematician.

Table 4.3

P	*Q*	*P* or *Q*	Not (*P* or *Q*)
T	T	T	**F**
T	F	T	**F**
F	T	T	**F**
F	F	F	**T**

- The negation of $P \vee Q$ turns out to be $(\neg P) \wedge (\neg Q)$. To prove that, use truth tables. You have to construct the table for $P \vee Q$ and then negate that column. (See Table 4.3.) Then, you have to do a second table where you do $\neg P$ and then $\neg Q$, and then you join them with "and." (See Table 4.4.) Hopefully, the final output looks the same.

- What is the negation of "*a* is odd or *b* is odd"? By De Morgan's laws, the negation is "*a* is not odd and *b* is not odd." The negation of the "or" statement turns into an "and" statement. In other words, *a* and *b* are both even.

Table 4.4

P	*Q*	Not *P*	Not *Q*	(Not *P*) and (Not *Q*)
T	T	F	F	**F**
T	F	F	T	**F**
F	T	T	F	**F**
F	F	T	T	**T**

Implication

- Most theorems in mathematics are implications: If *P*, then *Q* (hypothesis, then conclusion).

- If a triangle is equilateral, then it is isosceles. That's a true geometric theorem. If it's equilateral, then it has 3 congruent sides, and it's isosceles because it has 2 congruent sides. If a triangle has 2 equal angles, then it is isosceles.

- If *a* and *b* are even integers, then their sum $(a + b)$ is even. That is true. If *a* and *b* are odd integers, then their sum $(a + b)$ is odd. That is not true. For example, $7 + 3 = 10$, which is not odd. Therefore, that implication is false, and you just found a counterexample.

- If a function f is differentiable at a point, then it's continuous at a point. (It doesn't matter what those words mean, but the structure is important.) The notation for implication is usually $P \Rightarrow Q$, but there are many other notations—including "if P, then Q" and "P implies Q."

- When is an implication (such as "if P, then Q") true? Clearly, if both P and Q are true, then "P implies Q" is true. If P is true and Q is false, then "P implies Q" is false. However, what if the hypothesis, P, is false? It turns out that "P implies Q" is then always true. This might seem strange or counterintuitive, but mathematicians have accepted that if "P implies Q" is given and P happens to be a false hypothesis, then that implication turns out to be true.

- By constructing the truth table for $P \Rightarrow Q$, you can see that the only time $P \Rightarrow Q$ is false is in the case where P is true and Q is false. In particular, if the hypothesis is false, no matter what Q is, the implication $P \Rightarrow Q$ is true. In the third column, there is only 1 false, and it is in the second row. (See Table 4.5.)

Table 4.5

P	*Q*	*P* implies *Q*	*Q implies P*
T	T	**T**	**T**
T	F	**F**	**T**
F	T	**T**	**F**
F	F	**T**	**T**

- How does the truth table for $P \Rightarrow Q$ compare to the truth table of $Q \Rightarrow P$, which is called the converse of $P \Rightarrow Q$? In the truth table for $Q \Rightarrow P$, you reverse the roles of Q and P. In this truth table, the only bad case is when Q is true and P is false, and that occurs in the third row. These 2 truth tables are not the same. Therefore, the statement $P \Rightarrow Q$ is not equivalent to the statement $Q \Rightarrow P$. (See Table 4.5.)

- How do the truth tables for the following 2 statements compare? The first is the implication $P \Rightarrow Q$, and the second is $(\neg Q) \Rightarrow (\neg P)$. The columns are P, Q, $\neg Q$, $\neg P$, and then $(\neg Q) \Rightarrow (\neg P)$. In columns 3 and 4 ($\neg Q$ and $\neg P$), the only time it's false is if $\neg Q$ is true and $\neg P$ is false. That's the second row. The final fifth column turns out to be true, false, true, true—exactly the same as the original implication $P \Rightarrow Q$. Therefore, $P \Rightarrow Q$ is equivalent to $(\neg Q) \Rightarrow (\neg P)$. This is called a contrapositive, and it is the basis of proofs by contradiction. (See Table 4.6.)

Table 4.6

P	*Q*	Not *Q*	Not *P*	(Not *Q*) implies (Not *P*)
T	T	F	F	**T**
T	F	T	F	**F**
F	T	F	T	**T**
F	F	T	T	**T**

Equivalent Statements

- *P* and *Q* are logically equivalent to each other: *P* implies *Q*, and *Q* implies *P*. In other words, $P \Leftrightarrow Q$. Mathematicians will often say this as "*P* if and only if *Q*," which means if *P* is true, then *Q* is true, and if *Q* is true, then *P* is true. *P* and *Q* are logically equivalent if each implies the other. In particular, if one is true, then the other one is true, or if one of them is false, then the other one is false.

- Are $P \Rightarrow Q$ and $(\neg P) \vee Q$ equivalent to each other? To answer this, compare their truth tables. You already did the truth table for $P \Rightarrow Q$ (see Table 4.5), but for $(\neg P) \vee Q$, you need a column for *P*, *Q*, and $\neg P$ (which involves simply negating the first column). The column for $\neg P$ is false, false, true, true. Then, the fourth column is $(\neg P) \vee Q$, so look at the second and third columns: There will be a true statement everywhere, unless they are both false, which occurs in the second entry. It's the same column as $P \Rightarrow Q$, so these 2 statements are equivalent. (See Table 4.7.)

Table 4.7

P	*Q*	Not *P*	(Not *P*) or *Q*
T	T	F	**T**
T	F	F	**F**
F	T	T	**T**
F	F	T	**T**

- Are $\neg(P \vee Q)$, the negation of the disjunction $P \vee Q$, and $(\neg P) \vee (\neg Q)$ equivalent? You could do truth tables for both of them to show that they are not equivalent, or you could select a statement for *P* and a statement for *Q* and then compute all of the combinations. Let the statement P be the statement “2 is even,” which is true. Let Q be the statement “3 is even,” which is false. What is $P \vee Q$? That’s true because the first part is true. What is $\neg(P \vee Q)$? That’s false. The negation of a true statement is a false statement. What is $\neg P$? That’s false because P is true. What is $\neg Q$? That’s true now because Q is false. What is $(\neg P) \vee (\neg Q)$? That’s true. Hence, that statement is not equivalent to the previous one. You found a counterexample by picking some actual statements.

PROBLEMS

1. Construct the truth tables for $P \Rightarrow Q$ and $(\neg P) \Rightarrow (\neg Q)$. What do you observe?

2. Construct the truth tables for $\neg(P \vee Q)$ and $(\neg P) \wedge (\neg Q)$. What do you observe?

Existence and Uniqueness—Quantifiers

Lecture 5

This is the third and final lecture on mathematical logic. The theme of this lecture is the interplay between the quantifiers, or statements, "for all" and "there exists." In this lecture, in addition to learning about these 2 quantifiers, you will learn how to negate them—a process that becomes a bit complicated. These quantifiers occur throughout mathematics, but in particular, they occur in the field of sequences, which you will be introduced to in the second half of this lecture. As you will learn, it is pretty straightforward to determine whether a sequence has a limit, but proofs involving sequences can be quite unpleasant.

Quantifiers

- There are 2 quantifiers that will be the focus of this lecture: "for all" and "there exists." The quantifier "for all" means the following: Sometimes a statement is true for all values of the variable x. On the other hand, the quantifier "there exists" means the following: The statement is true for some values of the variable x but not necessarily for all of them. In other words, it's true for at least one value of the variable x.

- The "there exists" quantifier makes a claim about the existence of a solution, property, or object. It says that the statement is true for at least one value. For example, there exists a real number x such that $2x - 6 = 0$.

- The notation for the quantifier "there exists" is $\exists$. In mathematical textbooks, you'll see statements such as "$\exists x$ such that $2x - 6 = 0$." Then, you will see several abbreviations and symbols. For example, "$\exists x$ s.t. $2x - 6 = 0$." There's also a symbol, $\ni$, that stands for "such that." You'll sometimes see "$\exists x \ni 2x - 6 = 0$. Finally, textbooks will often drop the abbreviations and symbols and just put a comma into the statement: "$\exists x$, $2x - 6 = 0$."

- Is the following statement true? There exists an x such that $x^2 = -1$. If you're dealing with real numbers, it's not true because the square of any real number is positive, or perhaps 0 if x is 0. It's never negative. However, if you are dealing with complex numbers, it turns out that there does exist an x such that $x^2 = -1$. In fact, x is i, $\sqrt{-1}$. Of course, $-i$ also satisfies that equation.

- When you write statements such as "for all" and "there exists," make sure that you understand the underlying number system that is being addressed.

- The quantifier "for all" makes a claim about a statement being true for all values of x. For example, for all real numbers x, x^2 is nonnegative. That's a true statement. For every real number, x^2 is never negative; it's either 0 or positive.

- The notation for the "for all" quantifier is a similar notation as the notation for "there exists." It's $\forall$. A typical phrase from a mathematics textbook is as follows: $\forall x \in \mathbb{R}, x^2 \geq 0$. "For all real numbers, $x^2 \geq 0$" is a true statement.

- For example, for all real numbers x, $\sqrt{x^2} = x$. That is a false statement because if you square x and then take its square root, you do not always come back to x. For example, if x is -2, then x^2 is $(-2)^2$, or 4, but $\sqrt{4}$ is 2—not -2.

- Negations of "for all" statements involve "there exist" statements. The negation of "for all x, $P(x)$," where $P(x)$ is some statement, is "there exists x such that $\neg P(x)$ is true."

- For example, the negation of "all the cars in the parking lot are blue" is "there exists at least one car in the parking lot that is not blue." Furthermore, the negation of the statement "there exists a blue car in the parking lot" is "not one of the cars in the parking lot is blue." In other words, all the cars are different from blue.

- The negation of the statement “there exists x such that $P(x)$ is true” is “for all x, $\neg P(x)$ is true.” For example, the negation of the statement “there exists a real number x such that $x^2 = -1$” is “for all real numbers, $x^2 \neq -1$.”

- Sometimes with quantifiers, there are combinations. For example, the statement “for all real numbers x, there exists a real number y such that $y > x$” is true because no matter what real number x you pick, you always can find a y larger than the x you pick. There’s no largest real number.

- For all positive real numbers x, there exists a positive real number y such that $y < x$. Is that a true statement? For example, if you were to select x to be 5—a positive real number—can you find a y that is less than x? Let y be $x/2$, which is positive and smaller than x. This statement is true for any x that you choose.

Sequences

- Quantifiers play a very large role in calculus and precalculus when dealing with the concept of a sequence, which is a string of numbers. Sequences involving a first number, a second number, a third number, a fourth number, and so on—those that keep going—are infinite sequences.

- In the sequence 1, 2, 3, 4, 5 …, the first term is 1, the second term is 2, the third term is 3, and so on. Instead of approaching a fixed number, this sequence keeps going, getting larger and larger. Therefore, the sequence does not have a limit; it doesn’t approach a fixed number.

- In the sequence 1, 1/2, 1/3, 1/4, 1/5, …, the 50^{th} term is 1/50, and the 100^{th} term is 1/100. The terms of this sequence are approaching a fixed term; the terms are getting closer and closer to 0. They never reach 0, but they get really close to 0. Therefore, that sequence has a limit, and the limit is 0.

- Does the sequence 1, −1, 1, −1, 1, −1, … have a limit? Is it approaching a fixed number? It's kind of going back and forth between 2 different numbers—not settling down. Therefore, this sequence does not converge; it does not have a limit.

- In the Fibonacci sequence, the first two terms are 1 and 1, and then all the subsequent terms are obtained by adding the previous 2 together: 1, 1, 2, 3, 5, 8, 13, … . This sequence does not have a limit because the terms get bigger and bigger. It's not settling down and approaching a single fixed number.

- There is some notation for sequences. Textbooks usually use subscripts—for example, a_1, a_2, a_3—for the terms of the sequence, and they sometimes indicate the sequence by using curly brackets or braces: $\{a_n\}$.

- The sequence 1, 1/2, 1/3, 1/4, … converges to 0, and the notation for the limit of this sequence (0) is written as follows: $\lim_{n\to\infty} \frac{1}{n} = 0$. That statement says that the limit of that sequence equals 0. The sequence never actually reaches 0, but it gets as close to 0 as possible.

- With sequences, it's pretty easy to point out what the terms are and what the behavior is, but proving things about them can be quite difficult.

- What is the limit of the sequence $\{5 + 1/n\}$—if it exists? First, write out the first few terms: 5 + 1, 5 + 1/2, 5 + 1/3, 5 + 1/4 … . The $1/n$ part is decaying toward 0, so the limit is 5 + 0 = 5.

- What about the sequence $\{1/2^n\}$? The terms are 1/2, 1/4, 1/8 … . The limit is 0.

- What about the sequence $\{n/n + 1\}$? The terms are 1/2, 2/3, 3/4 … . The numbers are getting closer and closer to 1, so the limit is 1.

PROBLEMS

1. Is the following true or false? $\exists x > 0$ such that $\forall y>0$, $x > y$.

2. Write out the first 5 terms and find the limits of the sequences $\left\{\frac{n+1}{n}\right\}$ and $\left\{(-1)^n\right\}$.

The Simplest Road—Direct Proofs

Lecture 6

In this lecture, you will learn about direct proofs—the simplest kinds of proofs. The basic idea of direct proofs is that you begin with what is given to you (the hypothesis), you do some math (such as algebra), and you arrive at the conclusion. In this lecture, you will apply this technique of direct proofs to division and inequalities. Then, you will learn one of the tricks of mathematicians: the use of scratch paper to discover proofs.

Direct Proofs

- With direct proofs, you start with a hypothesis (some givens) and do some math (some algebra, some creativity) to arrive at a conclusion directly. You're showing that the statement P implies the statement Q—that the hypothesis P contains enough information to actually lead to the conclusion directly. The notation for this kind of proof is often $P \Rightarrow Q$.

- Let's do a direct proof of a theorem. The theorem is "the sum of 2 odd integers is an even integer." An even integer is of the form $2k$, where k is another integer (for example, 12 is 2×6, so 12 is even) whereas an odd integer is of the form $2k + 1$, or an even integer plus 1. For example, $7 + 9$ (2 odd numbers) $= 16$, which is even. This theorem seems like it's true, so let's do the proof.

- The hypothesis is that you have 2 odd numbers; let's call them $2k + 1$ and $2r + 1$, where k and r are integers. We want to prove that we can add them up and that their sum will be even. First, $(2k + 1) + (2r + 1) = 2k + 2r + 2$. Factoring the 2 out, we are left with $2(k + r + 1)$, which is 2 times an integer—$k + r + 1$—and that makes it even. In this proof, we were given the hypothesis that both numbers were odd, and we showed directly that the sum was even by just adding them together.

- Carl Gauss's formula for the sum of the first n positive integers is $\frac{n(n+1)}{2}$. To understand how that formula works, let's add the first 4 positive integers: 1 + 2 + 3 + 4 = 10. Using the formula, $\frac{4(4+1)}{2}$ = 20/2 = 10. It seems to be a true formula.

- Using the formula, the sum of the first 1000 positive integers is $\frac{1000(1000+1)}{2}$, which turns out to be 500,500. Let's prove the formula by using this example. Let x be the sum of the first 1000 integers: $x = 1 + 2 + 3 + 4 + \ldots + 999 + 1000$. Next, write this sum backward: $x = 1000 + 999 + \ldots + 4 + 3 + 2 + 1$. Then, add those 2 equations. To visualize the addition that is going on, stack the 2 equations on top of one another. On the left-hand side you get $x + x$, which is $2x$. Then, simple arithmetic results in the following.

$$x = 1 + 2 + \ldots + 999 + 1000.$$
$$x = 1000 + 999 + \ldots + 2 + 1.$$
$$2x = 1001 + 1001 + \ldots + 1001 + 1001.$$
$$2x = 1000(1001).$$
$$x = \frac{1000(1001)}{2}.$$

- To generalize this, instead of using 1000, use n. Let x be the sum $1 + 2 + \ldots + (n-1) + n$. Next, write it backward: $x = n + (n-1) + \ldots + 2 + 1$. Then, add those 2 equations. Again, to visualize the addition that is going on, stack the 2 equations on top of one another. On the left, you get $2x$. Then, simple arithmetic results in the following.

$$x = 1 + 2 + \ldots + (n-1) + n.$$
$$x = n + (n-1) + \ldots + 2 + 1.$$
$$2x = (n+1) + (n+1) + \ldots + (n+1) + (n+1).$$
$$2x = n(n+1).$$
$$x = \frac{n(n+1)}{2}.$$

Direct Proofs and Division

- Direct proofs are used in many different scenarios in mathematics, and one of those areas is division. If a and b are 2 integers, then a divides b ($a|b$) if there exists another integer k such that $ak = b$. For example, 3 divides 15 evenly because $3 \times 5 = 15$. In this case, the a is 3, the b is 15, and the k is 5. However, 3 does not divide 14 because 3 times no integer would result in 14. In other words, 3 doesn't divide evenly into 14; instead, it has a remainder.

- Directly prove the following theorem about division: If $a|b$ and $b|c$, then $a|c$, where a, b, and c are integers. For example, let $3|15$ be $a|b$ and $15|45$ be $b|c$. In this case, 3 divides 45 (a divides c). As a result, this theorem seems to be true; in mathematics, this is called a transitive property.

- To prove this theorem, first identify the hypothesis. In fact, there are 2 hypotheses: $a|b$ and $b|c$. The conclusion that you want to show is $a|c$. Start by translating the hypothesis into symbols and then playing with those symbols to see the conclusion pop out.

- To say that $a|b$ means that there exists some integer k such that $ak = b: a|b \Rightarrow ak = b.$ In the same fashion, $b|c$ means that there is some integer r such that $br = c: b|c \Rightarrow br = c.$ You want to end up with $a|c$, which really means that you want a times some integer to equal c. The second equation says that $c = br$. Now, you know what b is from the first equation; you can replace the b with ak. You now have the equation $c = ak(r)$. If you move the parentheses, you have $c = a(kr)$, which is the definition of $a|c$ because there exists an integer kr such that c equals a times kr. In other words, $c = br \Rightarrow c = (ak)r \Rightarrow c = a(kr).$ Hence, $a|c$.

Direct Proofs and Inequalities

- Inequalities play a huge role in mathematics, including in the areas of precalculus, calculus, and algebra. The notation $a < b$ just means that the number a is smaller than the number b. There are also other notations: $a \le b$, $a > b$, and $a \ge b$. For example, $-3 < 5$ and $\pi > 3$.

- Let's prove the following theorem: If a is less than b, then the conclusion is a is less than $(a + b)/2$, which in turn is less than b: $a < b \Rightarrow a < (a+b)/2 < b$. The hypothesis is $a < b$ (which are both real numbers). Because of the double inequality, in a sense there are 2 conclusions: $a < (a + b)/2$ and $(a + b)/2 < b$. Therefore, you have to prove 2 things. Do you believe that theorem? For example, $4 < 8$ implies $4 < (4 + 8)/2$, which is less than 8.

- Let's do the first part of the proof. Begin with $a < b$, and you want to show that a is less than the average $(a + b)/2$. Add a to both sides. By adding a to the left-hand side, you get $a + a = 2a$. On the right-hand side, you get $a + b$. Then, you have $2a < (a + b)$. Therefore, $a < b \Rightarrow 2a < (a+b) \Rightarrow a < (a+b)/2$.

- For the second part of the proof, you have to show that $(a + b)/2 < b$. Start with $a < b \Rightarrow (a+b) < 2b \Rightarrow (a+b)/2 < b$. Combining the first part of the proof, $a < (a + b)/2$, with the second part, $(a + b)/2 < b$, you get the triple inequality $a < (a + b)/2 < b$.

Working Backward

- A more difficult theorem to prove is: If $a < b$, then $4ab < (a + b)^2$. First, try some numbers. For example, $3 < 5$, so $a = 3$ and $b = 5$. Let's look at $4ab$, which would be $4(3)(5) = 60$. Is 60 less than $(3 + 5)^2$? Well, that's 8 squared, or 64. Yes, that's true.

- To prove this theorem, use some scratch paper. To discover the proof, start at the conclusion—what you're trying to prove—and play with it until it leads to the correct proof. On the scratch paper, write down what you want to prove: $4ab < (a + b)^2$. Doing some algebra, $(a + b)^2 = a^2 + 2ab + b^2$. Then, subtract $4ab$ from both sides: On the left side, $4ab - 4ab = 0$, and on the right side, $a^2 + 2ab + b^2 - 4ab = a^2 - 2ab + b^2$, so you are left with $0 < a^2 - 2ab + b^2$. Then, $a^2 - 2ab + b^2$ factors into $(a - b)^2$, so $0 < (a - b)^2$. This is a true statement.

- The correct proof is as follows.

$$a < b \Rightarrow a \neq b \Rightarrow 0 \neq a - b$$
$$\Rightarrow 0 < (a-b)^2$$
$$\Rightarrow 0 < a^2 - 2ab + b^2$$
$$\Rightarrow 4ab < a^2 + 2ab + b^2$$
$$\Rightarrow 4ab < (a+b)^2$$

PROBLEMS

1. Prove that if x and y are odd integers, then their product, xy, is also an odd integer.

2. Prove that $a < b < 0$ implies $a^2 > b^2$.

3. Consider the second-degree polynomial equation $ax^2 + bx + c = 0$, $a \neq 0$. Use the completing-the-square technique to derive the quadratic formula: $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Let's Go Backward—Proofs by Contradiction

Lecture 7

In this lecture, you will learn that $\sqrt{2}$ is irrational, and you will prove it using a very powerful technique—proofs by contradiction. In this technique, which is used throughout mathematics, you prove that a statement is true by supposing that the conclusion is actually false, and then you arrive at a contradiction. After you have proved that $\sqrt{2}$ is irrational, you will learn to apply this proof technique to other conjectures.

Direct Proofs versus Proofs by Contradiction

- Recall that the implication P implies Q is equivalent to the implication $\neg Q$ implies $\neg P$. The contrapositive is equivalent to P implies Q and it's a powerful way of proving theorems.

- Prove the following implication for natural numbers: If n^2 is even, then n is even. In other words, if the square of an integer is an even number, then the number itself is also an even number. Do you believe that this implication is true? Try some examples, and you'll see that it seems to be true. For example, 16 is even; it's a square (4^2), and 4 is even as well.

- To prove this implication, you have to first make sure that you are comfortable with even and odd integers. Recall that an integer is even if it's of the form $n = 2k$, where k is another integer. An integer is odd if it's of the form $2k + 1$.

- Attempt a direct proof of this theorem. Hypothesis: n^2 is even. Conclusion: n is even. Can you start with n^2 being even and directly get to the conclusion that n is even? Start by translating the fact that n^2 is even into symbols, so $n^2 = 2k$. You want to find out that n is even, but it's not clear how to proceed.

- Instead, try a proof by contradiction. The original direct proof hypothesis was P, and it is the statement "n^2 is even." The conclusion was "n is even," so that is Q, and P implies Q. What you want to prove "n^2 is even implies n is even." What is the contrapositive?

- First, $\neg Q$ is the statement "n is not even"—hence, it's odd—and $\neg P$ is the statement "n^2 is odd." In order to prove that P implies Q (that n^2 being even implies n being even), show that $\neg Q$ implies $\neg P$ (that n is odd implies that n^2 is odd). Assuming that n is odd, it will be of the form $2k + 1$, where k is an integer. Then, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$. That is odd because you can factor a 2 out of the first 2 terms: $2(2k^2 + 2k) + 1$. Therefore, n^2 is odd.

- If you want to prove that n^2 is even implies n is even, look at the conclusion: Either n is even, or it's not even. You want to prove it's even, so start by assuming that it's not—assume that it's odd. If it's odd, you get a contradiction: You get that n^2 is odd, and that contradicts the hypothesis that n^2 started as an even number. In fact, this is what is often called a proof by contradiction.

- The contrapositive $\neg Q$ implies $\neg P$ is not the same as the converse. The converse of $P \Rightarrow Q$ is $Q \Rightarrow P$, and those are not equivalent to each other. Proofs by contrapositive are closely related to proofs by contradiction.

- In that last proof, you wanted to show that if n^2 were even, then it could be concluded that n is even. The proof by contradiction would go like this. Assume that n is not even—that is, n is odd—then, you discovered that n^2 is also odd, and that's a contradiction with the original statement that n^2 was even.

- Here is the setup for a proof by contradiction. Suppose that you want to prove statement Q is true. Assume by way of contradiction that Q is false. If this leads—after some math—to some contradiction, perhaps with the hypothesis, then Q is in fact true.

The Square Root of 2

- A classic example of a proof by contradiction is the proof that $\sqrt{2}$ is irrational. Recall that a rational number, or fraction, is a quotient of 2 integers a/b, such as 2/3 or −12/75. This proof will show that $\sqrt{2}$ is not a fraction. The square root of 2 is that number whose square is equal to 2. On a calculator, it's about 1.414.

- There is a geometric interpretation of this proof. Recall the Pythagorean theorem: Given a right triangle *abc* with hypotenuse c and legs of length a and b, $a^2 + b^2 = c^2$. If you took the right triangle and let the 2 legs—a and b—have length 1, then the hypotenuse would be $1^2 + 1^2 = (\text{hypotenuse})^2$. The hypotenuse would be $\sqrt{2}$, which is going to turn out not to be a rational number.

- In this proof, you want to show that $\sqrt{2}$ is not rational—not a fraction. Start by assuming by way of contradiction that it is rational. That means that $\sqrt{2}$ equals the quotient of 2 integers a/b, where a and b are integers. You can assume further that these 2 integers a/b don't have any common factors. In other words, you can assume, by way of contraction, that $\sqrt{2}$ is equal to a/b and, furthermore, that a/b have been reduced to lowest terms.

- If $\sqrt{2}$ equals a/b, square both sides to get $2 = a^2/b^2$ and then multiply by b^2 to get the equation $2b^2 = a^2$.

- If $a^2 = 2b^2$, then that means that a^2 is even because it's 2 times an integer. You also just proved that if a^2 is even, then so is a. If a is even, then it can be rewritten as 2 times some other integer: $a = 2k$. If $2b^2 = a^2$, you can replace a with $2k$: $2b^2 = a^2 = (2k)^2 = 4k^2$. Canceling a common factor of 2, you are left with $b^2 = 2k^2$. Therefore, b^2 is also even because it equals 2 times something. If b^2 is even, then so is b.

- Because a and b are both even, the quotient a/b has a common factor of 2. You could have cancelled that 2 out. That's the contradiction. You started by saying that a/b was equal to $\sqrt{2}$ and that a and b didn't have any common factors. However, after doing some arithmetic, you discovered that a and b do have a common factor—2.

- You have now shown that $\sqrt{2}$ is irrational. You also can generalize it to $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, and so on. All of them turn out to be irrational.

More Proofs by Contradiction

- Prime numbers are numbers that only have 2 factors—1 and themselves. For example, 2, 3, 5, 7, and 11 are prime numbers. However, 6 is not a prime number because it has a factor of 2 and a factor of 3. By the way, 1 is not a prime number; the first prime number is 2.

- How many prime numbers are there? In *Elements*, Euclid stated that there are an infinite number of primes, and he proved it with a proof by contradiction. He started by assuming by way of contradiction that there is a finite number of primes. Then, he derived a contradiction. This will be proven in a later lecture.

- Prove the following theorem. The hypothesis is that the sum of 2 integers is odd; in other words, $a + b$ is odd. The conclusion is that a is odd or b is odd. The theorem that you want to prove is if $a + b$ is odd, then a is odd or b is odd.

- Do you believe this theorem? You could try some numerical examples. Try to prove it. The conclusion is a is odd or b is odd. The negation of that conclusion—an "or" statement—becomes an "and" statement. The negation of that conclusion is a and b are both even.

- Assume by way of contradiction that a and b are both even. That means that a is equal to $2k$ and that b is equal to $2r$. Each is 2 times an integer, and their sum would then be $2k + 2r$, which is $2(k + r)$. That is even, so it contradicts the hypothesis that $a + b$ is odd.

- Notice how similar this is to a proof by contrapositive. You negated the conclusion, did some math, and came to a contradiction—that $a + b$ is even. That contradicts the hypothesis because $a + b$ was assumed to be odd.

PROBLEMS

1. Prove that if n^2 is odd, then n is odd.

2. Prove that $\sqrt{3}$ is irrational. Hint: First show that if n^2 is a multiple of 3, then n is also a multiple of 3.

Let's Go Both Ways—If-and-Only-If Proofs

Lecture 8

If-and-only-if proofs occur all over mathematics. When you see a theorem that says "*P* if and only if *Q*," that means that *P* and *Q* are equivalent—that if one of them is true, then the other one is true as well, and if one of them is false, then so is the other. To prove a theorem of the form "*P* if and only if *Q*," 2 proofs are required: You have to go one way and then back the other way. You can also have more complicated situations with 3 or more statements involved.

If-and-Only-If Proofs

- A triangle is isosceles if it has 2 congruent sides—2 equal sides. If a triangle has 2 congruent sides, then it will also have 2 congruent angles. Conversely, if it has 2 congruent angles, it will have 2 congruent sides. This is an example of an if-and-only-if theorem. In a triangle, 2 sides are congruent "if and only if" 2 angles are congruent.

- A natural number is odd if and only if its square is odd. This statement actually involves 2 theorems: If the natural number is odd, then its square is odd, and if the square is odd, then the number itself is odd. Therefore, the phrase "if and only if" is a compact way of writing $P \Rightarrow Q$ and, simultaneously, $Q \Rightarrow P$.

- The phrase "if and only if" means that the 2 statements—*P* and *Q*, linked by *P* if and only if *Q*—are equivalent to each other. That is, the truth of one implies the truth of the other. Equivalently, the falseness of one statement implies the falseness of the other. If you have a theorem involving the phrase "if and only if," you have to show that $P \Rightarrow Q$ and then that $Q \Rightarrow P$.

- There are quite a few notations for "if and only if" in the literature. One of the most popular notations is "iff." A more old-fashioned notation is "*P* is necessary and sufficient for *Q*." The if-and-only-if phrase is often called a biconditional; it's a conditional, but it goes both ways. "P if and only if Q" means that these 2 statements, P and Q, are equivalent to each other. Each implies the other.

The Product of 2 Numbers

- If the product of 2 numbers is 0, then one of the numbers or the other one, or both, is equal to 0. In other words, $ab = 0$ if and only if $a = 0$ or $b = 0$. In algebra, the fact that a product equals 0 can help you determine the solutions to some polynomial equations.

- You want to prove that $ab = 0$ if and only if $a = 0$ or $b = 0$, so you have to show that if $ab = 0$, then $a = 0$ or $b = 0$. After you do that, you also have to show that if $a = 0$ or $b = 0$, then the product $ab = 0$. Therefore, there are 2 proofs that you have to do.

- If $a = 0$ or $b = 0$, then clearly the product is 0 because any number times 0 yields 0. If a is 0 or b is 0 or both are 0, then their product will also be 0. You have already proven the first half of the theorem.

- Next, assume that the product ab is equal to 0. You have to show that either $a = 0$ or $b = 0$. Assume that $ab = 0$ and consider a: It's either equal to 0, or it's not equal to 0. If it's equal to 0, then you are done. That's what you want to show. If it's not equal to 0, then you can do some algebra to discover that b is going to be 0.

- If a is 0, then the proof is done. If a is not 0, then take the original hypothesis $ab = 0$ and divide both sides by a. Because you are assuming that a is not 0, it's okay to divide, canceling the common factor. Then, $ab/a = 0/a$, which leads to $b = 0$.

Odd Numbers and Odd Squares

- A natural number (or positive integer) is odd if and only if its square is odd. For example, 9 is odd, so its square, 81, is odd. In addition, 4 is not odd, so its square, 16, is also not odd. In other words, the theorem that a is odd if and only if a^2 is odd is equivalent to the theorem b is even if and only if b^2 is even. That's the negation of both the phrases.

- You're going to show that if your number is odd, then its square is odd, and then you'll go in the other direction. Suppose that your number is n. The first direction is if n is odd, then try to show that n^2 is odd. This is a direct proof.

- Assume that n is odd. Then, it's of the form $2k + 1$, where k is an integer. Then, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$. Finally, $n^2 = 2(2k^2 + 2k) + 1$. Therefore, n^2 is odd because when you factor the 2 out, it's 2 times an integer $(2k^2 + 2k) + 1$, which makes it odd.

- Next, you have to go in the other direction. You have to show that if the square is odd, then the original number n is odd. Try a direct proof. Assume that n^2 is odd: $n^2 = 2k + 1$. That's what odd numbers look like, where k is an integer. Then, it is not clear how you should proceed.

- Instead, try a proof by contradiction. You are given that n^2 is odd, and assume by way of contradiction that n is not odd—rather, that it's even. That means that $n = 2k$. That's what even numbers look like. Then, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. That's an even number, but that's a contradiction. The hypothesis said that n^2 was odd, and you have concluded that it's even. Therefore, this proof by contradiction works, and you now have completed that if-and-only-if theorem.

Isosceles Triangles

- Given a triangle ABC, there's a geometric theorem that states that the angle at B is congruent to the angle at C if and only if side AB equals the length of side AC. That is, angles B and C are congruent if and only if the opposite sides are congruent (the length of side AB equals the length of side AC).

- The proof of this theorem uses 2 theorems from geometry: the side-angle-side (SAS) theorem and the angle-side-angle (ASA) theorem.

- For SAS, you're given 2 triangles, *ABC* and *DEF*. Suppose that *AB* is congruent to *DE*, angle *B* is congruent to angle at *E*, and side *BC* is congruent to side *EF*. The conclusion is that the 2 triangles are congruent, meaning that all 3 sides are the same length and all 3 angles are correspondingly congruent.

- For ASA, you're given 2 triangles, *ABC* and *DEF*. Suppose that angle *A* is congruent to angle *D*, *AB* is congruent to *DE*, and angle *B* is congruent to angle *E*. The conclusion is that the corresponding triangles are congruent.

- In this proof, you want to show that if a triangle has 2 congruent sides, then it has 2 congruent angles and that the converse is also true: Angle *B* is congruent to angle *C* if and only if side *AB* is congruent to side *AC*. You are going to show that triangle *ABC* is congruent to itself but in a different order. In other words, it's kind of flipped over on its back.

- First, suppose that the sides are congruent; suppose that *AB* is congruent to *AC*. Basically, one triangle is *ABC* and the other triangle is *ACB*. These are the same triangle, but the vertices are in a different order. With these 2 triangles, *AB* is congruent to *AC* because that's the hypothesis. The angle at *A* is, of course, congruent to itself. The third side, *AC*, is congruent to *AB*. Of course, that's the same hypothesis. Therefore, the triangles are congruent by SAS. Hence, the 2 triangles are congruent, but their vertices are in a different order. Triangle *ABC* is congruent to triangle *ACB*. That means that the angle at *B* is congruent to the angle at *C*.

- For the other direction, suppose that the 2 angles are congruent—angle *B* is congruent to angle *C*. You know that angle *B* is congruent to angle *C*, *BC* is congruent to *CB*, and angle *C* is congruent to angle *B*. This is ASA. Therefore, the triangles are congruent. That means that *AB* is the same length as *AC*.

A Triple If-and-Only-If Theorem

- Let x and y be 2 real numbers. You will show that the following 3 statements are equivalent: $x < y$, $x < (x + y)/2$, and $(x + y)/2 < y$. This means that if 1 of those statements is true, then the other 2 are also true. Therefore, any 1 of those 3 statements implies the other 2. Conversely, if 1 of those statements is false, then the other 2 statements are also false.

- Do you believe this theorem? Try some examples. If x is 4 and y is 10, then $(x + y)/2 = 14/2 = 7$. Therefore, it's true that x is less than y, that x is less than the average (7), and that the average is less than y (10).

- To prove this theorem, you have to show that each of the 3 statements is equivalent to the other 2. You will have to show that 1 implies 2, 2 implies 3, and 3 implies 1—that each 1 of these statements implies the other.

- To show that statement 1 implies statement 2, start with $x < y$ and show that x is less than the average, $(x + y)/2$.

$$x < y$$
$$2x < x + y$$
$$x < (x + y)/2.$$

- Next, show that 2 implies 3. You are given that x is less than the average, $(x + y)/2$, and you want to show that $(x + y)/2 < y$.

$$x < (x + y)/2$$
$$2x < x + y$$
$$2x + y < x + 2y$$
$$x + y < 2y$$
$$(x + y)/2 < y.$$

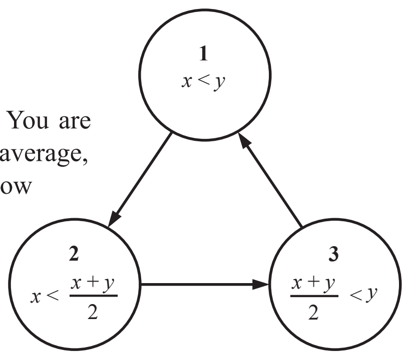


Figure 8.1

- The third and final step is to prove that 3 implies 1. You are given $(x + y)/2 < y$, and you want to show that $x < y$.

$$(x + y)/2 < y$$
$$x + y < 2y$$
$$x < y.$$

PROBLEMS

1. Prove that mn is odd if and only if both m and n are odd.

2. Let n be a natural number. Prove that n is divisible by 3 if and only if n^2 is divisible by 3.

The Language of Mathematics—Set Theory
Lecture 9

In this lecture, you will learn about elementary set theory—the language of mathematics. The language of set theory is a very common and important language tool for mathematicians. You will also learn how to manipulate sets through the use of unions, intersections, and complements. You will be introduced to the notion of subsets and the idea of an empty set. Perhaps most importantly, you will do a proof of how to show that 2 sets are equal to each other; the technique involves showing that each is a subset of the other.

Examples of Sets and Set Notation

- A set is nothing more than a collection of objects, such as the set of students in a class. If you are teaching, you have the set of students—for example, 35 students—in your class, and the set of boys in your class would be a subset of the set of all the students in your class.

- The set of all natural numbers = $N = \{1, 2, 3, \ldots\}$.

- The set of all integers = $Z = \{\ldots -2, -1, 0, 1, 2, \ldots\}$.

- The set of rational numbers = $Q = \{a/b | a, b \text{ integers}, b \neq 0\}$.

- The set of all real numbers = R.

- The set of all complex numbers = C.

- The objects in a set are called elements. The notation is $a \in A$, which means that a is an element of the set A.

- $4 \in N$ means that 4 is a natural number.

- $\pi \in R$ means that π is an element of the real numbers.

- $-3 \notin N$ means that –3 is not a natural number.
- $\sqrt{2} \notin Q$ means that $\sqrt{2}$ is not an element of the rational numbers.
- Mathematicians say that 2 sets are equal if they have the same elements. The world's smallest set is the empty set—the set that contains no elements—whose notation is Ø or { }. For example, what is the set of all real numbers satisfying the equation $x^2 = -1$? There are no real numbers satisfying that equation, so the answer is the empty set. Of course, if you were including complex numbers, then you'd have a different answer.
- Given 2 sets A and B, A is a subset of B if every element of A is also an element of B: $A \subseteq B$. For example, $N \subseteq Z \subseteq Q \subseteq R$.
- How do you prove that 2 sets are equal to each other? A very common mathematical technique is to show that each is a subset of the other. If A is a subset of B and B is a subset of A, then they must be equal to each other. Every element of A is in B, and every element of B is in A. Given 2 sets, if you want to show that they're the same, pick an element in the first set and show that it's in the second set and, conversely, pick an element in the second set and show that it's in the first set.

Operations on Sets

- The definition of a union of 2 sets is the set of all x's such that x is in A or x is in B: $A \cup B = \{x | x \in A \text{ or } x \in B\}$. For example, suppose that $A = \{1, 2, 5\}$ and $B = \{1, 5, 8\}$. The union of A and B is $\{1, 2, 5, 8\}$. Furthermore, suppose that $A = \{1, 2, 5\}$ and $C = \{1, 2, 5, 9, 12\}$. The union is the set C: $\{1, 2, 5, 9, 12\}$. If A is a subset of C, then the union of A and C is the larger set C.
- You can illustrate the idea of the union of 2 sets with a diagram called a Venn diagram, which is named after John Venn, who developed these diagrams around the 1880s.

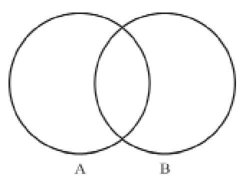


Figure 9.1

- The other major operation besides unions is the intersection of 2 sets, which involves the elements that are in the first set and are also in the second set. A intersects B is the set of all x's such that x is in A and x is in B: $A \cap B = \{x | x \in A \text{ and } x \in B\}$. Notice that the "and" is being used instead of the "or."

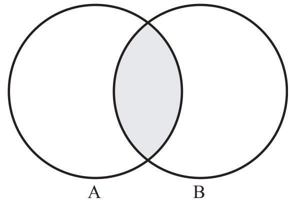


Figure 9.2

- For example, suppose that $A = \{1, 2, 5\}$ and $B = \{1, 5, 8\}$. Their intersection consists of 2 elements, 1 and 5: $\{1, 5\}$. Furthermore, suppose that $A = \{1, 2, 5\}$ and $C = \{1, 2, 5, 9, 12\}$. Then, their intersection is nothing more than A, the smaller set. Therefore, if A is a subset of C, then the intersection of A and C is A, the smaller set (whereas the union is the larger set).

- Suppose that $A = \{1, 2, 5\}$ and $D = \{6, 7, 9\}$. Because they don't have any common elements, the intersection is the empty set: $\{\ \}$.

- Begin with the set of real numbers, and let Q be the subset of rational numbers. The complement of Q consists of all the irrational numbers—all the numbers that are real numbers but aren't rational. For example, $\sqrt{2}$ would be in the complement; $\sqrt{2}$ is not a rational number, but it is a real number. Pi would be another one because pi turns out not to be a rational number.

- Consider the set of integers, and let N be the subset of natural numbers. The complement of N would be 0 and then all of the negative integers.

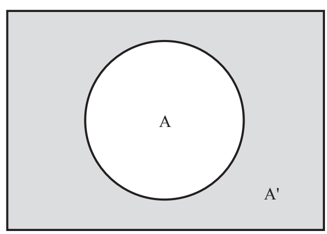


Figure 9.3

- There are various notations for complements in textbooks. The definition of a complement is if you have A, a subset of a universal set U, then the complement of A consists of all the elements in U that are not in A. The complement of A is all x's in U such that x

is not in A: $A' = \{x \in U \mid x \notin A\}$. For example, let $A = \{1, 2, 5\}$, a subset of the universal set, U, $\{1, 2, 3, 4, 5\}$. The complement of A is $\{3, 4\}$.

De Morgan's Laws

- How do you prove that 2 sets are the same? You show that each is a subset of the other. This technique can be illustrated with De Morgan's laws, which are named after the British mathematician Augustus De Morgan, who lived in the 1800s. Similar laws with the same name were used when dealing with "and" and "or" in the logic lectures.

- Imagine that you have some universal set U and 2 subsets A and B. The first law states that $(A \cap B)' = A' \cup B'$, and the second law states that $(A \cup B)' = A' \cap B'$.

- For example, suppose that the universal set is the positive integers 1 through 10: $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Let the subsets A and B be subsets of the set U. Let $A = \{2, 4, 6, 8\}$ and $B = \{1, 2, 3, 4, 5, 6, 7\}$.

  $A \cap B = \{2, 4, 6\}$.
  $(A \cap B)' = \{1, 3, 5, 7, 8, 9, 10\}$.
  $A' = \{1, 3, 5, 7, 9, 10\}$.
  $B' = \{8, 9, 10\}$.
  $A' \cup B' = \{1, 3, 5, 7, 8, 9, 10\}$.

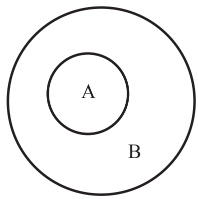


Figure 9.4

- To prove the first law, $(A \cap B)' = A' \cup B'$, apply the technique that shows that each is a subset of the other. Take an element in the first set and show that it's in the second set, and then take an element in the second set and show that it's in the first set.

- You want to prove that $(A \cap B)' = A' \cup B'$. Begin by taking an element, x, in the first set $(A \cap B)'$ and hope that you can find it in the second set. Then, choose an element in the second set and try to show that it's in the first set.

$$x \in (A \cap B)' \Rightarrow x \notin A \cap B$$
$$\Rightarrow x \notin A \text{ or } x \notin B$$
$$\Rightarrow x \in A' \text{ or } x \in B'$$
$$\Rightarrow x \in A' \cup B'.$$

$$(A \cap B)' \subseteq A' \cup B'.$$

$$x \in A' \cup B' \Rightarrow x \in A' \text{ or } x \in B'$$
$$\Rightarrow x \notin A \text{ or } x \notin B$$
$$\Rightarrow x \notin A \cap B$$
$$\Rightarrow x \in (A \cap B)'.$$

$$A' \cup B' \subseteq (A \cap B)'$$
$$(A \cap B)' = A' \cup B'.$$

- You've shown that an arbitrary element of the first set is in the second set and that an arbitrary element of the second set is in the first set. Therefore, these 2 sets must be the same.

Problems

1. Prove the other De Morgan's law: $(A \cup B)' = A' \cap B'$.

2. Let $U = \{a,b,c,x,y,z\}$, $A = \{a,b,x\}$, and $B = \{a,x,y\}$. Calculate $A \cup B$, $A \cap B$, A', $A \cup A'$, and $A \cap A'$.

Bigger and Bigger Sets—Infinite Sets

Lecture 10

Infinite sets are fascinating. In this lecture, you will learn that 2 sets can have the same size, or the same cardinality, but one can be a subset of the other. You will learn how to prove that the rational numbers, or the set of all fractions, is a countable set—just as the natural numbers are countable. In addition, you will learn how to show that the real numbers are not countable using a proof by contradiction.

Measuring the Size of Sets

- How do you measure the size of a set? When the set is finite, it's easy, but if it's infinite, it's much more difficult. If the set is finite, then you just have to match up the corresponding elements. For example, suppose that the set A consists of the numbers 1, 2, 3, and the set B consists of the letters x, y, z. Both sets have 3 elements. You can match these 2 sets up in the following fashion:1 is matched with x, 2 is matched with y, and 3 is matched with z. This is called a 1:1 correspondence because each item in one set corresponds to a unique element in the other set.

- The correspondence comes from the language of functions. Given 2 sets, a function $f: A \rightarrow B$ is a rule that assigns a unique element of B to every element of A, which is called the domain of that function. In the previous example, the domain was the set 1, 2, 3, and for each element in B, the element 1 went uniquely to x, the element 2 went uniquely to y, and 3 went uniquely to z.

- Examples of functions from algebra, precalculus, and calculus include exponential functions, logarithmic functions, and polynomials. For example, $f(x) = \sin x$ and $f(x) = x^2$.

- A function $f: A \to B$ is a bijection if for every element b in B, there is exactly one element a in A such that $f(a) = b$. In other words, every element is uniquely paired with another element in the other set. From the previous example, $f(1) = x$, $f(2) = y$, and $f(3) = z$.

- Are there any bijections between the following sets? $A = \{1, 2, 3, 4\}$, $B = \{x, y\}$, and $C = \{$dog, cat, bird, mouse, alligator$\}$. Because the first set has 4 elements, the second set has 2, and the third set has 5, there's no way to match them up so that each element gets matched to a unique element in the other set. You can't have a bijection with finite sets unless you have the same number of elements. In mathematics, a bijection is also called a one-to-one correspondence.

- Mathematicians say that 2 sets A and B have the same cardinality if there's a bijection $f: A \to B$. Sets with finite numbers of elements have no problem; they'll have the same cardinality if they have the same number of elements. Infinite sets are infinitely more interesting.

- Which set is bigger: the natural numbers, $N = \{1, 2, 3, 4, \ldots\}$, or the set of squares, $S = \{1, 4, 9, 16, \ldots\}$? Because S is a subset of N, S seems smaller, but there's a bijection between these 2 sets—a one-to-one correspondence—such that every positive integer, or natural number, is uniquely paired with a square. Each number in the first list is matched uniquely with each number in the second list. These 2 sets have the same cardinality.

- What about the cardinalities of N and Z? On one hand, Z, the integers, seems bigger than the natural numbers because the natural numbers are a subset of all the integers, but they have the same cardinality. You can match every natural number with a unique integer: 1 is paired with 0, 2 is paired with 1, 3 with –1, 4 with 2, 5 with –2, 6 with 3, and so on. There's a one-to-one correspondence between these 2 sets.

- The following function will yield the previous pattern:

  $$f(n) = \begin{Bmatrix} -(n-1)/2, n \text{ odd} \\ n/2, n \text{ even} \end{Bmatrix}.$$

  In other words, if n is odd, then $f(n)$ is $-(n-1)/2$, and if n is even, then $f(n)$ is $n/2$.

- A set is finite if it is either empty or has the same cardinality of the set $\{1, 2, 3, \ldots, n\}$. For example, the set $\{a, b, c\}$, which consists of 3 elements, has cardinality 3 because it's the same as the set $\{1, 2, 3\}$; in other words, you can match it up with a bijection to the set $\{1, 2, 3\}$.

- A set is infinite if it is not finite. An example is the set of natural numbers.

- A set is countably infinite if it has the same cardinality as the natural numbers. For example, the integers, the squares, and the even integers all have the same cardinality as the natural numbers.

- A set is countable if it is either finite or countably infinite. For example, the set of natural numbers is countably infinite, and the set $\{a, b, c\}$, consisting of 3 elements, is also countable.

- A set is uncountable if it is not countable. Are there uncountable sets? What about the set of rational numbers? There are many fractions; it's a very large set. A mathematical theorem states that the set of rational numbers, Q, is countably infinite. In other words, it's the same size as the natural numbers, even though the natural numbers are a seemingly small subset of all the fractions.

- To prove that the rational numbers are countably infinite, you have to have a bijection between the natural numbers and the tremendous number of fractions. Using what is known as the diagonalization argument, every rational number can be matched with a natural number. There is a one-to-one correspondence between the rational numbers and the natural numbers.

Uncountable Sets

- Are there any uncountable sets, or are all infinite sets countable? Do all infinite sets have the same cardinality as the natural numbers? The famous mathematician Georg Cantor, one of the mathematicians who put set theory together around the turn of the 20th century, showed that the real numbers are not countable—that they have different cardinalities. In fact, not just all the real numbers from minus infinity to plus infinity but, rather, the real numbers between 0 and 1 are uncountable.

- Recall that real numbers are decimals. On the open interval (0, 1), the real numbers are of the form $x = 0.d_1d_2d_3d_4 \ldots$. They are infinite decimals.

- Cantor claimed that the interval (0, 1) is uncountable. You will show that the open interval (0, 1) is uncountable by doing a proof by contradiction. Suppose, by way of contradiction, that there is a one-to-one correspondence, a bijection, between the natural numbers N and the real numbers on the interval (0, 1). Each real number has a decimal representation. Then, you're going to get a contradiction; hence, your supposition that the interval is countable will be false.

- In the proof, you suppose that there's a one-to-one correspondence between the natural numbers and all the real numbers, line up the real numbers, and then construct a number that's not on your list. That's the contradiction. Hence, you show that the cardinality of the interval (0, 1) is greater than the cardinality of the natural numbers.

- Then, it's an easy step to show that the cardinality of all the real numbers is also larger than the cardinality of the natural numbers. In fact, there's a one-to-one correspondence between the real numbers on the interval (0, 1) and all the real numbers. The one-to-one correspondence, the bijection, is the function $f(x) = \dfrac{2x-1}{x(x-1)}$. Because (0, 1) is uncountable, then all the real numbers are uncountable.

- The cardinality of (0, 1) is equal to the cardinality of the real numbers. The cardinality of the real numbers is greater than the cardinality of the natural numbers. Is there a set of real numbers in between all the real numbers and just the natural numbers with a different cardinality? Cantor conjectured that there probably is no set of real numbers whose cardinality is strictly between that of the natural numbers and the real numbers. This is called the continuum hypothesis, one of the great hypotheses of all mathematics.

- In 1931, a Princeton mathematician named Kurt Gödel showed that it's impossible to disprove the continuum hypothesis from the axioms of set theory. In 1963, a mathematician at Stanford named Paul Cohen showed that it's impossible to prove the continuum hypothesis from the axioms of set theory. In other words, it's independent of the axioms of set theory. There are 2 alternative versions of set theory—one in which the continuum hypothesis is true and one in which it's false—and both are equally valid theories of set theory.

PROBLEMS

1. Show that the set of even positive integers is countably infinite.

2. Why is the set of all irrational numbers uncountable?

Mathematical Induction

Lecture 11

This is the first of 3 lectures on mathematical induction, a very powerful tool for proving theorems involving positive integers, or natural numbers. A mathematical induction proof has 2 steps: the base case and the induction step. As you will learn in this lecture, the base case usually involves proving your theorem for $n = 1$, but sometimes the base case is something different than 1. In addition, you will once again experience how useful scratch paper can be.

Proofs by Induction

- Mathematical induction is used for proving theorems involving the natural numbers, or the positive integers. There are 2 steps to mathematical induction. First, you show that the property is true for 1, the first natural number, which is called the base case. Then, you do the induction step, which involves assuming that the property is true for the natural number n and trying to therefore show that it is true for $n + 1$.

- If you've done both of those steps—the base case and the induction step—then because it's true for 1, it's true for 1 + 1, or 2, and because it's true for 2, it's true for 2 + 1, or 3, and so on. Hence, your property is true for all natural numbers.

- Using mathematical induction, prove Gauss's famous formula, which is that the sum of the first n positive integers is $\frac{n(n+1)}{2}$. Recall that you did a direct proof of this formula in Lecture 6.

- What is the sum of the first 5 natural numbers? Using the formula, $\frac{n(n+1)}{2} = \frac{5(5+1)}{2}$ = 30/2 = 15. Now that you understand how the formula works, do the mathematical induction proof of the base case. You have to show that the formula is true when $n = 1$. Does $1 = \frac{n(n+1)}{2}$ in the case when $n = 1$? Yes, $\frac{1(1+1)}{2}$ = 2/2 is 1. The formula is valid in the base case.

- Next, assume that the theorem is true for n and try to show that it's true for $n + 1$. In this proof, you are allowed to use the formula for the case n—the fact that $1 + 2 + 3 \ldots + n = \frac{n(n+1)}{2}$. The next step is for the sum to now go out to $n + 1$. The formula used to be $\frac{n(n+1)}{2}$, but because n is now increased by 1, the formula becomes $\frac{(n+1)(n+2)}{2}$. Therefore, you're trying to prove that $1 + 2 + 3 \ldots + n + (n + 1) = \frac{(n+1)(n+2)}{2}$.

- For this proof, you will start with the left-hand side of what you want to prove and, by doing some algebra, end up with the right-hand side. The first thing to notice is that the summation out to $n + 1$ can be split into 2 pieces. First, the summation goes out to n, and then there's one more term, $n + 1$. The summation out to n is part of the induction hypothesis, so you are allowed to replace that with the formula $\frac{n(n+1)}{2}$. The right-hand becomes $\frac{n(n+1)}{2}$ + $(n + 1)$. By mathematical induction, the following formula is true for all natural numbers.

$$1+2\,...+n+(n+1)=\frac{n(n+1)}{2}+(n+1)$$

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

$$=\frac{1}{2}[n(n+1)+2(n+1)]$$

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

$$=\frac{(n+1)(n+2)}{2}.$$

- The formal statements for mathematical induction are as follows. Let $P(n)$ be a statement about natural numbers. To show that $P(n)$ is true for all natural numbers 1, 2, 3, …, you have to do 2 things. First, you have to prove $P(1)$; you have to verify the base case—that your formula is true when $n = 1$. Then, you have to prove that for each natural number n, if $P(n)$ is true, then $P(n + 1)$ is true. The key is that you are allowed to use the formula for the case n as you're trying to prove it for $(n + 1)$.

Summation Formulas

- In this example, you're going to play with some numbers, and then you're going to guess a formula. Then, you're going to prove the formula using mathematical induction. Add the following string of odd numbers.

  1 = 1.
  1 + 3 = 4.
  1 + 3 + 5 = 9.
  1 + 3 + 5 + 7 = 16.

- What do you observe? Can you guess the formula? It looks like if you add the first 4 odd numbers, you get 4^2. If you add the first 5 odd numbers, you get 5^2. Odd numbers are of the form $2k + 1$, but they can also be of the form $2k - 1$, which is more useful here.

- Based on the data, the formula that you want to prove is $1 + 3 + 5 + 7 + \ldots (2n - 1) = n^2$. Do you believe this formula? Do some examples. If n is 1, then the summation is the first term, 1, and that equals 1^2. If n is 2, then the summation is $1 + 3$ (because $2n - 1 = 3$), and that equals 2^2 because $1 + 3 = 4$, which equals 2^2. You could try some more examples, and you would see that this indeed is the correct formula.

- To prove that this is the correct formula, you want to prove that $1 + 3 + 5 + \ldots (2n - 1) = n^2$. First, prove the base case: Is the formula true when n is 1? The left-hand side ends up being 1, and the right-hand side is 1^2. They are equal, so you have proved the base case.

- For the induction step, you are allowed to assume that the formula is valid for n. In other words, you're allowed to assume the formula $1 + 3 + 5 + \ldots (2n - 1) = n^2$. You want to prove the next case, $(n + 1)$, which is the next odd number in the series.

- First, the summation out to $(2n + 1)$ can be split into the sum out to $(2n - 1)$ and then the final term $(2n + 1)$. The sum out to $(2n - 1)$ can be replaced by the formula n^2 because that's the case n. By replacing the entire sum out to $(2n - 1)$ with n^2, the sum becomes $n^2 + (2n + 1)$. Finally, $n^2 + 2n + 1$ is a perfect square and can be factored into $(n + 1)^2$.

  $P(n + 1)$: $1 + 3 + 5 + \ldots + (2n - 1) + (2n + 1) = (n + 1)^2$
  $1 + 3 + 5 + \ldots + (2n - 1) + (2n + 1) = [1 + 3 + \ldots + (2n - 1)] + (2n + 1)$
  $= n^2 + (2n + 1)$
  $= n^2 + 2n + 1$
  $= (n + 1)^2$.

- There are many summation formulas, and many of them are crucial in calculus. The following formula is the sum of the first n squares: $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$. Do you believe this formula? For example, the sum of the first 10 squares is $1 + 4 + 9 + 16 + \ldots + 10^2$. According to this formula, the sum is $\frac{10(11)(21)}{6} = 385$. You can prove this formula by using mathematical induction.

- Another summation formula is the sum of the first n cubes: $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$. You can check this formula with a few examples, and of course, it can be proven with mathematical induction.

- Sometimes, a mathematical induction theorem is not true necessarily at 1; instead, it might only be true for values larger than 12, for example. In other words, the base case might be a case that is different than $n = 1$. The principle is the same, however.

A More Challenging Example

- The following is a more challenging example that illustrates a case in which the base case is not necessarily $n = 1$. You're going to guess the formula first, and then you'll prove it. Find an inequality relating 2^n and n^2.

- To start, let n be 1: $2^1 > 1^2$. If n is 2, then $2^2 = 2^2$. If n is 3, then $2^3 < 3^2$, or $8 < 9$. The sign changed from a greater-than sign to an equals sign to a less-than sign, so there doesn't seem to be much of a pattern. If n is 4, then $2^4 = 4^2$, or $16 = 16$. If n is 5, $2^5 > 5^2$, or $32 > 25$. If n is 6, $2^6 > 6^2$, $64 > 36$.

- If you keep going, you'll see that from this point on, 2^n is indeed greater than n^2, so your theorem for the moment is $2^n > n^2$ for $n > 4$. The base case is 5 because you know you can't prove the theorem for the earlier cases. Indeed, $2^5 > 5^2$. Next is the induction step, in which you assume that your theorem is true for n and try to prove it for $n + 1$. You're allowed to use $2^n > n^2$ and $n > 4$ in your proof.

- Using scratch paper, play around with the conclusion, and hopefully, that will give rise to the proof. You want to prove $2^{n+1} > (n + 1)^2$, which results when you replace n with $n + 1$.

$$
\begin{aligned}
2^{n+1} &> (n+1)^2 \\
2 \times 2^n &> n^2 + 2n + 1 \\
n^2 + n^2 &> n^2 + 2n + 1 \\
n^2 &> 2n + 1 \\
n \times n &> 2n + 1 \\
4n &> 2n + 1 \\
2n &> 1.
\end{aligned}
$$

- The final statement, $2n > 1$, is a true statement. If you can start your proof with that true statement and reverse the steps that you just did on your scratch paper, then the proof might work. The proof of $2n > 1$ is as follows.

$$
\begin{aligned}
2n &> 1 \\
4n &> 2n + 1 \\
n^2 &> 2n + 1 \\
2n^2 &> n^2 + 2n + 1 \\
2 \times 2^n &> (n+1)^2 \\
2^{n+1} &> (n+1)^2.
\end{aligned}
$$

PROBLEMS

1. Use induction to prove the summation formula $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

2. Use induction to prove that for all positive integers, $n \le 2^n$.

Deeper and Deeper—More Induction
Lecture 12

As you will learn in this lecture, mathematical induction can be used in many areas of mathematics. In this lecture, you will apply mathematical induction to a number of areas, including inductive definitions, which involve using induction to define a concept. In addition, you will develop both finite and infinite geometric series using induction. Furthermore, you will learn how induction can play a large role when dealing with set theory and division theorems.

Using Induction to Define Mathematical Concepts

- Sometimes, mathematical induction is used to define mathematical concepts. For example, factorials play a role in many mathematical subjects.

  $1! = 1.$
  $2! = 2 \times 1 = 2.$
  $3! = 3 \times 2 \times 1 = 6.$
  $4! = 4 \times 3 \times 2 \times 1 = 24.$
  $5! = 5 \times 4 \times 3 \times 2 \times 1.$

- Notice that 5! is also $5 \times 4!$. Therefore, if you know what 4! is, then 5! is an easy computation. In fact, that leads to the inductive definition of factorial (!): 1! is defined to be 1 (which is the base case), and $n!$ is defined to be $n(n-1)!$.

- Geometric series are studied in many algebra and calculus courses. For example, in the geometric series $1+\frac{1}{2}+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^3+\cdots+\left(\frac{1}{2}\right)^n$, each term is multiplied by the same factor of 1/2, which is r, the common multiplier.

- Suppose that you want to prove the following formula: For $r \neq 1$ and n, a positive integer, $1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}$. Suppose that r is 1/2 and that n is 8.

$$1 + \frac{1}{2} + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^3 + \cdots + \left(\frac{1}{2}\right)^8$$

$$= \frac{1 - \left(\frac{1}{2}\right)^9}{1 - \frac{1}{2}} = \frac{1 - \frac{1}{512}}{\frac{1}{2}} = \frac{511}{256} = 2 - \frac{1}{256}.$$

- Notice in this formula that the numerator is $1 - r^{n+1}$, and in this case, that equals $(1/2)^9$, which is a pretty small number. In fact, it's 1/512. Imagine that instead of adding 8 terms, you add 1 billion terms. That r^{n+1} gets smaller and smaller and, in fact, approaches 0 as a limit. If you add more and more terms, you are left with the following result: $1 + 1/2 + (1/2)^2 + (1/2)^3 + \ldots = 1/(1 - 1/2) = 2$. This is an infinite geometric series, and its sum is 2. Another way to write the formula for the sum of an infinite geometric series is as follows.

$$\sum_{n=0}^{\infty} \left(\frac{1}{2}\right)^n = \left(\frac{1}{2}\right)^0 + \left(\frac{1}{2}\right)^1 + \left(\frac{1}{2}\right)^2 + \cdots + \left(\frac{1}{2}\right)^n + \cdots$$

$$= 1 + \frac{1}{2} + \frac{1}{4} + \cdots = 2.$$

- You want to prove the sum of the finite geometric series $1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}$, where r is not equal to 1, by using mathematical induction. The base case is $n = 0$ because that's the first term. Therefore, when n is 0, it's r^0, which is 1—and that, in fact, works in the formula.

$$1 = \frac{1 - r^{0+1}}{1 - r} = \frac{1 - r}{1 - r} = 1.$$

- For the induction step, assume that the formula is true for n and show that it's true for the case $n + 1$. You want to prove the following: $1+r+r^2+\cdots+r^n+r^{n+1}=\dfrac{1-r^{n+2}}{1-r}$. Start with the left-hand side and try to prove that it equals the right-hand side. The proof is as follows.

$$
\begin{aligned}
1+r+r^2+\cdots+r^n+r^{n+1} &= \frac{1-r^{n+1}}{1-r}+r^{n+1} \\
&= \frac{1-r^{n+1}+r^{n+1}-r^{n+2}}{1-r} \\
&= \frac{1-r^{n+2}}{1-r},\ r\neq 1.
\end{aligned}
$$

- What happens if the formula you just proved is an infinite geometric series? When r was 1/2, then r^{n+1} becomes very small as n becomes larger. In a sense, the term disappears if you have an infinite number of terms. That will always be true if r is between –1 and 1. If r is a small fraction, such as 1/3 or –1/2, then when you raise it to a large power, it becomes smaller and smaller. If you restrict r to be between –1 and 1, the term r^{n+1} disappears in the formula for the summation of an infinite geometric series: $1 + r + r^2 + r^3 + \ldots + r^n + \ldots = 1/(1- r)$, $-1 < r < 1$.

- What does 0.99999… mean? It can be thought of as 0.9 + 0.09 + 0.009 + … . In fractions, this can be written as $\dfrac{9}{10}+\dfrac{9}{10}\left(\dfrac{1}{10}\right)+\dfrac{9}{10}\left(\dfrac{1}{10}\right)^2+\ldots$. This is a geometric series with the common value, or a, of 9/10. Then, r is 1/10, which is less than 1 in absolute value.

$$
\begin{aligned}
0.999\ldots &= 0.9+.09+.009+\ldots \\
&= \frac{9}{10}+\frac{9}{10}\left(\frac{1}{10}\right)+\frac{9}{10}\left(\frac{1}{10}\right)^2+\ldots \\
&= \frac{a}{1-r}=\frac{\frac{9}{10}}{1-\frac{1}{10}}=\frac{\frac{9}{10}}{\frac{9}{10}}=1.
\end{aligned}
$$

- This proof shows that 0.9999… equals 1. Do you believe it? If 0.9999… is not equal to 1, what else could it be? For example, 0.33333… equals 1/3. If you believe that, multiply both sides by 3, and then you get that 0.99999… equals 1. Note that 1 and 0.99999… are 2 decimal representations of the same real number.

Mathematical Induction and Set Theory

- Mathematical induction can be applied to set theory. For example, how many subsets does a finite set have? To approach this problem, start by doing an example.

- A 1-element set has 2 subsets: itself and the null set. All sets are subsets of themselves, and the empty set, or null set, is a subset of every set. A 2-element set, $\{a, b\}$, has 4 subsets: $\{a, b\}$, $\{a\}$, $\{b\}$, and $\{\ \}$. A 3-element set, $\{a, b, c\}$ has 8 subsets: $\{a, b, c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$, $\{a\}$, $\{b\}$, $\{c\}$, and $\{\ \}$. The pattern, or theorem, is if your set has n elements, then it will have 2^n subsets. This is what you want to prove.

- You can write those 8 subsets in a different way. First, you can write the 4 subsets that don't contain the letter c: $\{a, b\}$, $\{a\}$, $\{b\}$, and $\{\ \}$. Then, there are 4 subsets that do contain the letter c: $\{a, b, c\}$, $\{a, c\}$, $\{b, c\}$, and $\{c\}$. Consider the 4 sets without the c to be matched up with the 4 sets with the c. This is the idea of the proof.

- For the proof of this theorem, the base case, $n = 1$, has 2 subsets: $\{a\}$ and $\{\ \}$. For the induction step, assume that the theorem is true for any set with n elements. Given any set $\{a_1, a_2, \ldots, a_n\}$, you are allowed to assume that the set has 2^n subsets. You have to show that it's true for $n + 1$.

- Consider a set, S, with $n + 1$ elements: $S = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$. You need to show that S has 2^{n+1} subsets. There are 2^n subsets of S that do not contain the element a_{n+1}. Ignoring the final element, a_{n+1}, you are dealing with a set of n elements, and by the induction hypothesis, it has 2^n subsets. In total, there are 2^n subsets that do not contain a_{n+1} and 2^n subsets that do contain a_{n+1}. Therefore, $2^n + 2^n = 2(2^n) = 2^{n+1}$.

Mathematical Induction and Division

- Recall that an integer a divides an integer b ($a|b$) if there is another integer c such that $ac = b$. For example, 4 divides 12 because $4 \times 3 = 12$. In addition, 3 does not divide 7; 3 is not a factor of 7.

- The following is a property of division: If $a|b$ and $a|c$, then $a|(b + c)$. You can try some examples to show that it's true. Using mathematical induction, prove the following divisibility theorem: $3|(n^3 - n)$ for $n > 1$.

- Do you believe the theorem? If you try some examples, you'll see that it's always true. For example, if $n = 4$, then $4^3 - 4 = 64 - 4 = 60$, and 3 does divide 60.

- The base case, $n = 2$, is true because $2^3 - 2 = 8 - 2 = 6$, and 3 divides 6. Next, you have to assume that the theorem is true for n and try to show that it's true for $n + 1$. You want to show that $3|[(n + 1)^3 - (n + 1)]$. In other words, you want to show that 3 is a factor of that expression. Assume that $3|(n^3 - n)$ and analyze $(n + 1)^3 - (n + 1)$.

$$\begin{aligned}(n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - (n+1) \\ &= n^3 - n + (3n^2 + 3n) \\ &= (n^3 - n) + 3(n^2 + n).\end{aligned}$$

- It may not look like it at first glance, but 3 is a factor of each of these final 2 terms. It is clearly a factor of the second term, and it is a factor of the first term because the induction hypothesis states that you are allowed to assume that 3 divides $n^3 - n$. Hence, 3 divides the sum $(n + 1)^3 - (n + 1)$.

PROBLEMS

1. Use mathematical induction to prove that $2|\left(n^2 + n\right)$.

2. Prove the divisibility property: If $a|b$ and $a|c$, then $a|(b+c)$.

Strong Induction and the Fibonacci Numbers

Lecture 13

In this third and final lecture on mathematical induction, you will learn about strong induction, which is a more powerful version of regular mathematical induction. With strong induction, you can use the fact that the theorem or statement that you want to prove is valid not only for n, but also for all previous values—down to the base case. In this lecture, you will use strong induction to prove 2 theorems: One of the theorems involves factoring integers into their prime factors, and the other involves the famous Binet formula, with which you can compute any Fibonacci number without having to compute the previous ones.

Strong Mathematical Induction

- As a review, the main ideas of mathematical induction are as follows. In order to prove a statement involving the positive integers, you have to do 2 things. First, you have to verify the base case, which is usually $n = 1$. Then, assuming your statement is true for n, you must show that it's true for $n + 1$.

- Strong mathematical induction modifies the second step—the induction step: You're allowed to assume that the statement you're trying to prove is true for all natural numbers up to n. Then, you try to prove that it's true for $n + 1$. In other words, when you're trying to prove the statement $P(n + 1)$, you can assume that $P(n)$ is true and that all the previous statements—such as $P(n - 1)$, $P(n - 2)$, and all the way down to the base case—are true.

- Recall that you can take a positive integer and factor it into its prime factors. A natural number is a prime number if it is greater than 1 and if its only factors are 1 and itself. For example, 2, 3, 5, and 7 are all prime numbers. However, remember that 1 is not considered a prime number.

- In theory, you can factor natural numbers into their prime factors. For example, $15 = 3 \times 5$, $12 = 2 \times 2 \times 3$, and $125 = 5^3 = 5 \times 5 \times 5$. This is the idea of the following theorem. Every integer $n > 1$ can be expressed as a finite product of primes. In other words, given any arbitrary positive integer, you can express it as a finite product of prime numbers. You are going to prove this theorem using strong induction.

- The base case $n = 2$ is already factored into primes because 2 is a prime number. Next, assume that the theorem is true for all values up to n. That is, assume that any natural number between 2 and n can be expressed as a finite product of primes.

- Start by considering $n + 1$ and proving that it is also a product of primes. If $n + 1$ is a prime number, then you are done because it's factored into a product of primes. However, if it's not a prime number, then it must have some devisor q because it's not a prime number. Therefore, $n + 1 = q \times r$, where q is one factor and r is the other factor; hence, the product qr yields $n + 1$. The key point is that q and r are natural numbers greater than 1 but less than n.

- By the strong induction hypothesis, q and r, being less than n, both can be expressed as a product of primes (or they are primes themselves). Hence, $n + 1$, which equals $q \times r$, is a product of primes. It's the product consisting of the primes that yield q times the primes that yield r. For this proof, you needed to use strong mathematical induction because when you factored $n + 1$, you obtained 2 numbers that were not equal to n—they were probably much smaller than n—and you needed to know that any number less than or equal to n could be factored into primes.

- To illustrate the proof, suppose that $n + 1 = 104$. Then, determine whether 104 is a prime number. Because it is not a prime number, then it must have some factors that are smaller than 104. For example, $n + 1 = 104 = 4 \times 26$. By strong induction, 4 and 26 are both products of primes ($4 = 2 \times 2$ and $26 = 2 \times 13$). Hence, 104 is a product of primes.

- This result is closely related to the fundamental theorem of arithmetic, which states that any integer greater than 1 can be uniquely written as a product of primes—except perhaps for order. For example, 12 = 2 × 2 × 3 and 12 = 3 × 2 × 2; these 2 are not counted as being different.

- In other words, this theorem states that given a positive integer, you can factor it into primes, but it's done in a unique manner. There's only one way to do it. That's much harder to prove. Furthermore, factoring large integers is actually quite difficult to do in practice.

The Fibonacci Sequence and the Binet Formula

- The terms of the Fibonacci sequence are 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, … . The rule is that a given Fibonacci number is equal to the sum of the previous 2 Fibonacci numbers. Here's the formal definition of the Fibonacci sequence. The first number, f_1, is equal to 1, and f_2 is also equal to 1. From the first 2 terms on, there is a recursive definition: f_{n+1} is defined to be $f_n + f_{n-1}$. According to the rule, $f_3 = f_2 + f_1 = 1 + 1 = 2$ and $f_4 = f_3 + f_2 = 2 + 1 = 3$.

- Known as the golden ratio, phi $(\phi) = \frac{1+\sqrt{5}}{2} \approx 1.618$. In addition, $\alpha = \frac{1-\sqrt{5}}{2} \approx -0.618$. Given phi and α, the formula for the n^{th} Fibonacci number is as follows: $f_n = \frac{\phi^n - \alpha^n}{\sqrt{5}}$. This formula, known as the Binet formula, is named after the French mathematician Jacques Binet of the 19th century.

- To prove that the Binet formula yields the Fibonacci numbers, you need a few lemmas, which are theorems that are solely needed for a proof.

- The first lemma states the following: $\phi^2 = \phi + 1$. You can directly prove this lemma as follows.

$$\phi^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{4+2+2\sqrt{5}}{4}$$

$$= \frac{4}{4} + \frac{2+2\sqrt{5}}{4} = 1 + \frac{1+\sqrt{5}}{2} = 1 + \phi.$$

- The second lemma looks similar to the first one: $\alpha^2 = \alpha + 1$, where α is $\frac{1-\sqrt{5}}{2}$.

- In order to prove the Binet formula, you have to prove 2 base cases: Verify that the formula is true for $n = 1$ and for $n = 2$. Then, use strong induction.

- Start by verifying that the formula $f_n = \frac{\phi^n - \alpha^n}{\sqrt{5}}$ holds for f_1, the first Fibonacci number, which is 1.

$$f_1 = \frac{\phi^1 - \alpha^1}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}}$$

$$= \frac{\frac{(1+\sqrt{5})-(1-\sqrt{5})}{2}}{\sqrt{5}} = \frac{\frac{2\sqrt{5}}{2}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1.$$

- Because f_1 is true, the formula is verified in the first base case. Then, to prove that f_2, which is also equal to 1 according to the formula, is true, you must use the 2 lemmas as follows.

$$f_2 = \frac{\phi^2 - \alpha^2}{\sqrt{5}} = \frac{(\phi+1)-(\alpha+1)}{\sqrt{5}} = \frac{\phi - \alpha}{\sqrt{5}} = 1.$$

- The formula is now verified for the first 2 Fibonacci numbers. Next is the strong mathematical induction step: Assume that the formula is true for all numbers up to *n*. Therefore, the next step is to prove that the formula is true for *n* + 1.

$$f_{n+1} = \frac{\phi^{n+1} - \alpha^{n+1}}{\sqrt{5}}.$$

- Using some algebra and both lemmas, you can prove the famous Binet formula as follows.

$$\begin{aligned} f_{n+1} = f_n + f_{n-1} &= \frac{\phi^n - \alpha^n}{\sqrt{5}} + \frac{\phi^{n-1} - \alpha^{n-1}}{\sqrt{5}} \\ &= \frac{1}{\sqrt{5}}\left[\phi^n + \phi^{n-1} - \left(\alpha^n + \alpha^{n-1}\right)\right] \\ &= \frac{1}{\sqrt{5}}\left[\phi^{n-1}(\phi+1) - \alpha^{n-1}(\alpha+1)\right] \\ &= \frac{1}{\sqrt{5}}\left[\phi^{n-1}(\phi^2) - \alpha^{n-1}(\alpha^2)\right] \\ &= \frac{1}{\sqrt{5}}\left(\phi^{n+1} - \alpha^{n+1}\right) = \frac{\phi^{n+1} - \alpha^{n+1}}{\sqrt{5}}. \end{aligned}$$

- Notice that you needed strong induction because when you were analyzing f_{n+1}, you wrote it as $f_n + f_{n-1}$, so you needed to know that both of those could be replaced with the formula by the induction hypothesis. In addition, remember that you proved the formula for 2 base cases. If you're going to prove the formula for f_3, you're going to have to know that it's true for f_2 and f_1.

- Given the Fibonacci sequence, how would you find the 100th Fibonacci number? Using the Binet formula, a calculator can be used to calculate the 100th term in the Fibonacci sequence: $\dfrac{\phi^{100} - \alpha^{100}}{\sqrt{5}} = 354,224,848,179,261,915,07.$

PROBLEMS

1. Illustrate the proof that every integer greater than 1 can be expressed as a product of primes using the integers 95 and 96.

2. Prove that if $\alpha = \frac{1-\sqrt{5}}{2}$, then $\alpha^2 = \alpha + 1$.

I Exist Therefore I Am—Existence Proofs

Lecture 14

In this lecture, you will learn about existence proofs, or proofs by construction. These involve theorems that declare that a certain mathematical object exists. Many times, you prove something exists because you actually construct it. However, an existence proof might not actually exhibit the object but, instead, determine only that it exists. In this lecture, you will encounter a very subtle problem concerning irrational numbers.

Existence Proofs

- A class of theorems called existence theorems declares that a certain object or property exists. Many times, an existence theorem tells you that a certain property exists, but it does not necessarily tell you what it equals.

- There are many examples in mathematics of existence theorems. Suppose that you have a polynomial function that, evaluated at 0, equals –1, and evaluated at 1, equals 2. In other words, if f is the polynomial, then $f(0) = -1$ and $f(1) = 2$. Why does f have a root, or sometimes called a zero, in the interval [0, 1]? For example, graph the polynomial $x^3 + 2x - 1$, which satisfies those properties.

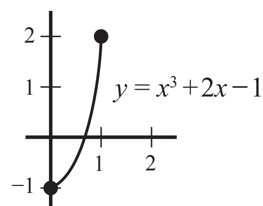


Figure 14.1

- Graphs of polynomials are continuous; they don't have any breaks in them. Because of this, you can be confident that in between 0 and 1, there's some value x such that $f(x) = 0$. This polynomial has at least 1 root in the interval [0, 1].

- Suppose that you are given 2 distinct rational numbers, or fractions. Does there always exist a third rational number in between them?

How could you prove it, given the rational numbers a and b such that $a > b$?

- For example, suppose that $a = 2$ and $b = 1.99$. Can you think of a rational number in between those 2 rational numbers? All terminating decimals are rational numbers, and 1.999 is between 1.99 and 2.

- In general, can you prove that given any 2 distinct rational numbers, there exists a third rational number between them? This is an existence theorem that was actually proved in a previous lecture. The average, $\frac{a+b}{2}$, is in between the 2 numbers a and b.

- The set of rational numbers is quite dense; between any 2 rational numbers there is always a number in between. However, the rational numbers are countable; they can be put in a one-to-one correspondence with the natural numbers.

- Consider polynomials of degree 2, which are called quadratic polynomials. In general, they are in the form $ax^2 + bx + c = 0$, assuming that a is nonzero. The theorem is that there are always 2 roots to a quadratic polynomial. These 2 roots might be the same, or they might be complex numbers. This is another existence theorem.

- Examples of this theorem are as follows.

    - $x^2 + 3x + 2 = (x+2)(x+1) = 0 \Rightarrow x = -2, -1.$
    - $x^2 + 2x + 1 = (x+1)(x+1) = 0 \Rightarrow x = -1, -1.$
    - $x^2 + 1 = 0 \Rightarrow x = i, -i.$

- In each of these 3 examples, you could find the solutions using the famous quadratic formula, which tells you the roots that x equals given a quadratic polynomial.

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Proving Existence Theorems

- Recall that the rational numbers are the fractions. Another category of numbers is called the algebraic numbers. An algebraic number is a real number that is a root to a polynomial equation with integer coefficients. For example, $\sqrt{2}$ is not a rational number, but it is an algebraic number because it is a root to the following polynomial having integer coefficients: $x^2 - 2 = 0$.

- The rational numbers are a subset of the algebraic numbers, so all rational numbers are algebraic. The real numbers can be divided into the rational numbers and the irrational numbers, but another way to divide them is into the algebraic numbers and the numbers that aren't algebraic, which are called transcendental numbers.

- In the 1800s, Joseph Liouville proved the existence of the transcendental numbers by constructing one. It's an infinite decimal, like all real numbers: 0.11000100…1000…1000… .

- Since then, mathematicians have been able to prove that numbers such as pi and e are transcendental. Strangely, the sum pi + e is not necessarily transcendental. It is an unsolved problem; nobody knows if that sum is transcendental or algebraic.

- One way to prove an existence theorem is by exhibiting or constructing at least one object that satisfies the theorem. However, some existence theorems are proven without actually constructing the object.

- The fundamental theorem of algebra is an existence theorem that states that if $f(x)$ is a polynomial of degree $n > 0$, then f has at least one zero in the complex number system. This was first proved by Gauss in 1799 when he was only 22 years old.

- The intermediate value theorem for polynomials is another existence theorem, and it states that if f is a polynomial defined on the closed interval $[a, b]$ and k is a number between $f(a)$ and $f(b)$, then there exists at least one number c in the interval $[a, b]$ such that $f(c) = k$.

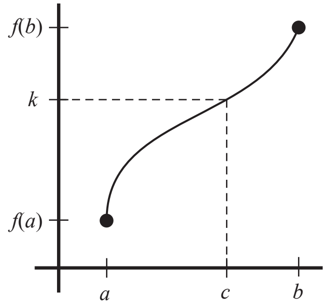


Figure 14.2

- How do you prove this theorem?
It is a difficult proof that is usually proven in advanced calculus courses. You can apply this theorem to the polynomial $x^3 + 2x - 1$, for example. It satisfies the property that $f(0)$ is -1 and $f(1)$ is 2. According to the intermediate value theorem, f will have a 0 in the interval $[0, 1]$.

- In the graph of that cubic polynomial, at $x = 0$, the value of the polynomial is -1. At $x = 1$, the value of the polynomial is 2, so it's going from -1 to 2 along the y-axis, and every value in between -1 and 2 is attained on the polynomial. In other words, if you pick k to be 0 in the intermediate value theorem, then there is some c value in the interval $[0, 1]$ such that $f(c) = 0$. The polynomial has to cross the x-axis.

- To find this zero, you could use the formula for cubic polynomials, but that is an unpleasant formula. In practice, you may not need the exact answer. You can use your calculator, which probably has a capability of approximating zeros of functions, to get an answer of approximately 0.453.

- The following is another existence theorem: There exists 2 irrational numbers, a and b, such that a^b is rational. This proof requires some knowledge of exponents.

- Recall the following facts about exponents.

$$a^{b^c} = a^{\left(b^c\right)}.$$
$$\left(a^b\right)^c = a^{bc}.$$

- The following numerical examples will help demonstrate the previous exponential properties.

$$2^{3^2} = 2^{\left(3^2\right)} = 2^9 = 512.$$
$$\left(2^3\right)^2 = 2^{3\times 2} = 2^6 = 64.$$
$$\left(2^3\right)^2 = 8^2 = 64.$$

- Consider $x = \left(\sqrt{2}\right)^{\sqrt{2}}$. This number x is an irrational number raised to an irrational power. However, is x rational or irrational? If x is rational, then you are done. If x is rational, then you have constructed an irrational raised to an irrational power, and the output is rational.

- However, if x is irrational, consider the following.

$$x^{\sqrt{2}} = \left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\times\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2.$$

- In either case—whether x is rational or irrational—you obtain the construction that you desired: an irrational number raised to an irrational power yielding a rational number. In either case, you are able to prove the theorem without knowing whether x is rational or irrational. Using some high-powered mathematics, it turns out that x is irrational, but that's not needed for this proof.

Nonexistence Proofs

- Nonexistence proofs claim that something does not exist. For example, the quadratic formula is used for second-degree polynomials. In addition, there is a cubic formula for third-degree polynomials and a formula for fourth-degree polynomials. However, given an arbitrary fifth-degree polynomial, there is no general formula for solving it.

- In fact, mathematicians have proven that no such formula will ever exist. It's called the Abel-Ruffini theorem of 1824. Mathematicians were looking for a formula for fifth-degree polynomials for hundreds of years and never could find one. Finally, this nonexistence proof showed that mathematicians never will find one. In graduate-level mathematics, you might prove this theorem.

PROBLEMS

1. Let x be an irrational number, and let a and b, $b \neq 0$, be rational. Prove that $a + bx$ is irrational.

2. How many zeros does the function $f(x) = x^3 - 2x^2 - x + 1$ have?

3. Show that there exist 2 irrational numbers a and b such that a^b is irrational.

I Am One of a Kind—Uniqueness Proofs

Lecture 15

In the last lecture, you learned about existence proofs, which involve proving whether a mathematical object exists. Given that an object exists, how many objects exist with that property? Existence and uniqueness theorems occur all over mathematics and, generally, there are 2 things to prove in such theorems: existence and uniqueness. Something might exist, but is it unique? In this lecture, you will learn how to prove that something is unique—specifically, by assuming that it's not unique and deriving a contradiction. Proofs by contradiction will play a major role in this lecture.

Proving Uniqueness

- Given that something exists, is it unique? To prove that something is unique, you would need to do a proof by contradiction. You would assume that there is more than 1 and then, hopefully, derive a contradiction. In other words, you would assume that 2 objects satisfy the statement and then show that, in fact, those 2 objects are the same.

- There are many examples from mathematics that are existence and uniqueness theorems. For example, the fundamental theorem of arithmetic states that any integer greater than 1 can be written as a unique product of prime numbers. In a previous lecture, you used strong mathematical induction to show that given any positive integer, you can write it as a product of prime numbers. The uniqueness part requires a separate proof that is much more difficult.

- A theorem from linear algebra states that if a square matrix has an inverse, then that inverse is unique. For example, a square matrix, or a 2×2 matrix, contains the entries $\begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$. If you claim that the inverse is the matrix $\begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}$, you mean that if you were to multiply those 2 matrices together using matrix multiplication, you would obtain the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The inverse of a matrix is a matrix that, when multiplied by the given matrix, produces the identity matrix.

- The proof that the inverse of a matrix is unique is part of every linear algebra course. In fact, the uniqueness of inverses in other settings is a standard proof in mathematics. How would you do the proof? Given a matrix, assume it has 2 inverses or more and derive a contradiction from that supposition. That's a proof by contradiction.

- Beginning calculus deals with limits, and a typical limit expression is in the form of the following: $\lim_{x\to 2}(x+2)=4.$ In other words, the limit of the quantity (x + 2) as x approaches 2 equals 4. With the function (x + 2), as x gets closer and closer to 2, x + 2 gets closer and closer to 4. The uniqueness part is that if that limit exists, it is unique. Functions have at most 1 limit.

- The following is a more complicated limit problem from elementary calculus: $\lim_{x\to 2}\frac{x^2-4}{x-2}=?$. What's the limit? Take values of x near 2, such as 1.999 and 2.001. Then, evaluate the expression $\frac{x^2-4}{x-2}$, and you'll discover that the function gets closer and closer to 4. Both the numerator and denominator vanish when x = 2, but with limits, you never actually worry about the value at the number you're approaching. You only care about what is happening as you get very close to that number.

- To understand why the answer is 4, use algebra to factor and solve the following.

$$\lim_{x\to 2}\left(\frac{x^2-4}{x-2}\right)=\lim_{x\to 2}\left(\frac{(x-2)(x+2)}{x-2}\right)$$

$$=\lim_{x\to 2}\left(\frac{x+2}{1}\right)=\lim_{x\to 2}(x+2)=4.$$

Uniqueness and Algebra

- Let x be a real number that is different from 0 and 1. Prove that there exists a unique real number y such that $y/x = y - x$.

- For example, suppose that $x = 2$. What is y? If y is 4, then $4/2 = 2$ and $4 - 2 = 2$. Is there another value of y that would work? Is 4 a unique value? You have to show that it's unique.

- Because you can't divide by 0, x can't be 0. In addition, x cannot be 1 because if x were equal to 1, then you would have $y/1 = y - 1$, or $y = y - 1$, which can't happen.

- For the existence proof, you want to show that given x, where x is not equal to 0 or 1, then there exists a unique y such that $y/x = y - x$. Use algebra to solve for y.

$$\begin{aligned} y - x &= \frac{y}{x} \\ yx - x^2 &= y \\ yx - y &= x^2 \\ y(x-1) &= x^2 \\ y &= \frac{x^2}{x-1}. \end{aligned}$$

- Then, try a few examples to see if the formula seems to work.
  - $x = 2 \Rightarrow y = \dfrac{2^2}{2-1} = 4.$
  - $x = 3 \Rightarrow y = \dfrac{3^2}{3-1} = \dfrac{9}{2}.$

- Is this value of y unique? To show uniqueness, assume that it's not unique and then show that it leads to a contradiction or that, in fact, it is. Assume that there's a y value that works and also a z value. Assume that y and z both satisfy the equation $y/x = y - x$ and $z/x = z - x$. Then, you have to show that $y = z$.

$$\frac{y}{x} = y - x \Rightarrow x = y - \frac{y}{x}$$

$$\frac{z}{x} = z - x \Rightarrow x = z - \frac{z}{x}$$

$$y - \frac{y}{x} = z - \frac{z}{x} \Rightarrow yx - y = zx - z$$

$$\Rightarrow y(x-1) = z(x-1) \Rightarrow y = z.$$

- You assumed that there were 2 solutions, y and z, and showed that they are, in fact, equal to each other. In this problem, you showed that a solution exists. You derived a formula for it and then showed that it is unique.

The Division Algorithm

- The division algorithm states the following: Let a and b be positive integers. Then, there exists unique integers q and r such that $a = bq + r$, where $0 \le r < b$. This theorem is an existence and uniqueness theorem. Prove the existence and uniqueness for q and r, the quotient and the remainder.

- There are many different existence proofs for this theorem. Some are based on long division. One of them uses mathematical induction. The uniqueness part of the proof is the interesting part, and that is what you will prove.

- Suppose that $a = 34$ and $b = 6$. To find the quotient, q, use a calculator or long division to obtain the following: $34 = 6 \times 5 + 4$. The quotient is 5, and the remainder is 4. The key is that 4 is greater than or equal to 0 and less than 6. The uniqueness part of this theorem states that the q and the r are unique given any 2 positive integers.

- To prove the uniqueness part of this theorem, you have to show that q and r are unique. Assume they aren't unique. You're given a and b, 2 fixed numbers, and you're going to assume that there exist 2 different quotients, q and q', and 2 different remainders, r and r'. You will ultimately show that $r = r'$ and $q = q'$.

- In the division algorithm, you're assuming that the q and the r are not unique—that perhaps there is another set, q' and r', that also satisfies the algorithm. Given a and b, assume there exist q, q', r, and r' such that $a = bq + r = bq' + r'$, where $0 \le r < b$ and $0 \le r' < b$. Your goal is to show that $r = r'$ and $q = q'$.

- You have 2 remainders, r' and r. One of them is greater than the other or equal to the other. Assume without loss of generality that r' is greater than or equal to r. In other words, you could take r' to be greater than or equal to r, or you could take r to be greater than or equal to r'. It doesn't make any difference; it won't change the proof.

$$a = bq + r, 0 \le r < b.$$

$$a = bq' + r', 0 \le r' < b.$$

$$bq + r = bq' + r'$$

$$\Rightarrow bq - bq' = r' - r$$

$$\Rightarrow b(q - q') = r' - r.$$

b divides $r' - r$.

Since $r' \ge r$, $0 \le r' - r$.

Since $r' < b$, $r' - r < b$.

Hence, $0 \le r' - r < b$.

b divides $r' - r$ and $0 \le r' - r < b$.

$$r' - r = 0 \Rightarrow r' = r$$

$$\Rightarrow b(q - q') = 0 \Rightarrow q = q'.$$

- In this uniqueness proof, you showed uniqueness by the typical argument—by assuming that there were 2 q's and 2 r's that worked in the division algorithm. Then, you showed that, in fact, there was only 1 remainder and 1 quotient with the restriction of the remainder being between 0 and b.

Uniqueness and Set Theory

- Show that there is a unique set B such that for every set A, $A \cup B = A$. How could you prove uniqueness? Assume that it's not unique. Assume that there is a B and a C that satisfy the theorem: $A \cup B = A$ for all A and $A \cup C = A$ for all A.

- In the first equation, let $A = C$: $C \cup B = C$. In the second equation, let $A = B$: $B \cup C = B$. Hence, $C = B$.

- What is the set B that is satisfied? The empty set satisfies this theorem.

PROBLEMS

1. Apply the division algorithm to the numbers $a = 503$ and $b = 9$.

2. Show that the equation $x^2 + 2x + 1 = 0$ has a unique solution.

Let Me Count the Ways—Enumeration Proofs

Lecture 16

In this lecture, you will learn that one way to prove a theorem is to break it into pieces, or cases. Sometimes, the cases are pretty obvious, but with some theorems—such as the triangle inequality theorem, which you will encounter in this lecture—things become a little more complicated. In particular, you will learn about the famous 4-color theorem, which was proved by cases. Often, proofs by enumeration, or proofs by cases, are not thought of as being very elegant, but they are valid.

Proofs by Enumeration

- Proofs by enumeration, or cases, are those in which the truth of a statement is established by considering all of the possible cases. Many times, it's not considered very elegant by mathematicians, but it's a perfectly valid proof technique.

- For any positive integer n, $n^2 + n$ is even. Is this true? Try some examples. For example, $5^2 + 5 = 30$, which is even, and $6^2 + 6 = 42$, which is also even. You could try some more examples, and you would find that it always yields an even number.

- To prove this theorem by cases, start by considering 2 cases: n is even or n is odd. In each case, prove the theorem. First, suppose that n is even, which means that n is 2 times some other integer—$2k$, for example. Then, evaluate $n^2 + n$ and see if it's even. Because it turns out to be 2 times an integer, you have proven the theorem for the first case.

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

- The second case states that n is odd, which means that it is in the form $2k + 1$. Evaluate $n^2 + n$ in this case. You will find that it is an even number.

$$\begin{aligned} n^2 + n &= (2k+1)^2 + (2k+1) \\ &= 4k^2 + 4k + 1 + (2k+1) = 4k^2 + 6k + 2 \\ &= 2(2k^2 + 3k + 1). \end{aligned}$$

- In each case, you verified that $n^2 + n$ is an even number.

- Let n be a positive integer that is greater than 1. Prove that when n^2 is divided by 4, the remainder is either 0 or 1. Recall that when you divide n^2 by 4, the division algorithm states that the remainder can be between 0 and 4. In this case, you're claiming that the remainder is just 0 or 1; it's never 2, and it's never 3.

- To prove this theorem, start with some examples. If $n = 2$, then $n^2 = 4$, and when you divide that by 4, there's no remainder, so the remainder is 0. If $n = 3$, then $n^2 = 9$, and when you divide by 4, the remainder is 1. If $n = 4$, then $n^2 = 16$, which has a remainder of 0 when divided by 4. If $n = 5$, then $n^2 = 25$, which has a remainder of 1 when divided by 4. If n is even, the remainder seems to be 0, and if n is odd, the remainder seems to be 1.

- The cases are that n is even or n is odd. Prove those 2 cases. For n to be even in case 1, that means that $n = 2k$, where k is an integer. Then, n^2 is $4k^2$, and when you divide that by 4, the remainder is 0.

- For n to be odd in case 2, that means that $n = 2k + 1$, which leads to $4k^2 + 4k + 1 = 4(k^2 + k) + 1$. The remainder is 1 when you divide $4k^2 + 4k + 1$ by 4.

The Triangle Inequality Theorem

- The triangle inequality theorem states that for all real numbers a and b, the absolute value of the sum $a + b$ is less than or equal to the absolute value of a plus the absolute value of b: $|a + b| \leq |a| + |b|$.

- The absolute value of a number is always going to be nonnegative. If the number is negative, then an absolute value symbol rips off the minus sign and turns it into a positive number. If the number is positive, then it already equals its absolute value.

$$|a| = \begin{cases} a, & a \geq 0 \\ -a, & a < 0 \end{cases}.$$

- Prove the triangle inequality by cases. First, play with some examples to see if you can figure out what the cases are going to be. Suppose that both numbers are positive—for example, $a = 3$ and $b = 5$. Compute both sides of the inequality. Then, suppose that both numbers are negative and compute both sides of the inequality.

$$a = 3, b = 5:$$

$$|a+b| = |3+5| = |8| = 8.$$

$$|a| + |b| = |3| + |5| = 3 + 5 = 8.$$

$$a = -3, b = -5:$$

$$|a+b| = |-3+(-5)| = |-8| = 8.$$

$$|a| + |b| = |-3| + |-5| = 3 + 5 = 8.$$

- Next, suppose that $a = 3$ and $b = -5$.

$$a = 3, b = -5:$$

$$|a+b| = |3+(-5)| = |-2| = 2.$$

$$|a| + |b| = |3| + |-5| = 3 + 5 = 8.$$

- Finally, briefly compute the trivial case in which one of the 2 numbers is 0.

$$a = 0, b = -7:$$

$$|a+b| = |0-7| = 7.$$

$$|a| + |b| = 0 + |-7| = 7.$$

- If the 2 numbers a and b have the same sign, then there's equality. If they have different signs, then there's inequality. Finally, if one number is 0, the whole thing is trivial.

- Prove the triangle inequality by breaking your observations into cases. First, disregard the case when a or b is 0 because the theorem is automatic there. The remaining cases are: both positive, both negative, one positive, and one negative.

- Case 1: Suppose that a and b are both positive, which means that their sum is positive: $|a + b| = a + b$ and $|a| + |b| = a + b$. There is equality in this case.

- Case 2: If a and b are both negative, then their sum is also negative: $|a + b| = -(a + b) = (-a) + (-b)$ and $|a| + |b| = (-a) + (-b)$. There is also equality in this case.

- Case 3: Without loss of generality, you can say that a is positive and b is negative because it doesn't matter which one is positive and which one is negative.

- There are 2 subcases within this case. The first subcase is $a + b \geq 0$.

$$|a+b| = a+b < a-b$$
$$= a + (-b) = |a| + |b|.$$

$$|a+b| < |a| + |b|.$$

- The second subcase is $a + b < 0$.

$$|a+b| = -(a+b)$$
$$= (-a)+(-b) < a+(-b) = |a|+|b|.$$

$$|a+b| < |a|+|b|.$$

- In all 3 cases and both subcases, you verified the triangle inequality. There are other proofs of this theorem, which occur in many math courses, including calculus and linear algebra.

The 4-Color Theorem

- Given a map with many countries, how many colors will it take to color the map so that adjacent countries have different colors? Are 4 colors enough to paint any conceivable map? How would you prove this?

- There are an infinite number of maps; you can imagine maps with a billion countries. Therefore, this seems like an infinite problem. It was proposed by Francis Guthrie in 1852, and then in 1879, a proof was published by Alfred Kempe. However, 11 years later, Percy Heawood showed that the proof by Kempe had an error. Heawood then worked on this problem and proved the 5-color theorem. The 4-color theorem was finally proven in 1976 by 2 mathematicians at the University of Illinois.

- This was the first major theorem of mathematics in which the proof was done using computers. The 2 mathematicians were able to reduce this problem to a finite number of cases. There were an infinite number of maps, but they had some very fancy techniques that reduced it to 1936 cases.

- Then, they attacked each case in turn and showed that the theorem held in all of those cases. This was a proof based on cases. When this theorem was proven, it was done with a lot of computer time, and many mathematicians didn't believe it right away because they couldn't check the math themselves. Today, the proof is considered valid, and mathematicians believe the 4-color theorem.

Enumeration and Cubes

- In this example, you will analyze some data, generate a theorem, and then prove it.

$$1^3 = 1.$$
$$2^3 = 8 = 9 - 1.$$
$$3^3 = 27 = 9(3).$$
$$4^3 = 64 = 9(7) + 1.$$
$$5^3 = 125 = 9(14) - 1.$$
$$6^3 = 216 = 9(24).$$
$$7^3 = 343 = 9(38) + 1.$$
$$8^3 = 512 = 9(57) - 1.$$

- With these numbers, a pattern emerges: If you take the cube of a number and then divide it by 9, the remainder is either 0, 1, or –1. Furthermore, multiples of 3 have a remainder of 0; multiples of 3 + 1, such as 4 or 7, have a remainder of 1; and multiples of 3 – 1, such as 2 and 5, have a remainder of –1. You can prove this by cases.

- The theorem is that every positive integer that is a perfect cube is either a multiple of 9, 1 more than a multiple of 9, or 1 less than a multiple of 9. The integer either has a remainder of 0, a remainder of 1, or a remainder of –1.

- Case 1: $n = 3k$. Case 2: $n = 3k + 1$. Case 3: $n = 3k + 2$ (or you could use $3k - 1$). These 3 cases cover all integers. In each case, cube n and see what happens.

$$
\begin{aligned}
n &= 3k \\
n^3 &= 27k^3 = 9\left(3k^3\right).
\end{aligned}
$$

$$
\begin{aligned}
n &= 3k+1 \\
n^3 &= \left(3k+1\right)^3 = 27k^3 + 27k^2 + 9k + 1 \\
&= 9\left(3k^3 + 3k^2 + k\right) + 1.
\end{aligned}
$$

$$
\begin{aligned}
n &= 3k+2 \\
n^3 &= \left(3k+2\right)^3 = 27k^3 + 54k^2 + 36k + 8 \\
&= 27k^3 + 54k^2 + 36k + 9 - 1 \\
&= 9\left(3k^3 + 6k^2 + 4k + 1\right) - 1.
\end{aligned}
$$

PROBLEMS

1. Let x and y be real numbers. Use proof by cases to show that $\left|\frac{x}{y}\right| = \frac{|x|}{|y|}$.

2. Let m and n be 2 integers not divisible by 3. Use proof by cases to show that mn is not divisible by 3.

Not True! Counterexamples and Paradoxes

Lecture 17

Instead of proving conjectures, in this lecture, you will learn about counterexamples—how to prove that a statement or conjecture is false. Proofs can be long and complicated, but a single example can be a counterexample that proves that the conjecture is false. In addition, you will learn about some famous paradoxes, which are wonderful problems in mathematics that often don't have a simple answer. After learning about these paradoxes, you might even be encouraged to explore more on your own.

Proving Conjectures False

- How would you show that a conjecture is false? For example, is $(a + b)^2 = a^2 + b^2$ correct for every possible value of a and b?

- How can you prove that there are some values of a and b that make the theorem false? Try to discover a value for a and a value for b that render the equation false.

- For example, let $a = 1$ and $b = 1$. Then, $(1 + 1)^2 = 2^2 = 4$, which clearly does not equal $1^2 + 1^2$. That is a simple example. It is a counterexample.

- Basically, given a conjecture or statement, proving it can be difficult. All of the previous techniques that you have learned can be used to try to prove statements, but it's actually much easier to disprove a conjecture. All you have to do is find a single counterexample.

- Consider $n^2 - n + 41$ for various values of the integer n. In each of the following examples, it seems that you get a prime number as the output—but will it always yield a prime number?

  $1^2 - 1 + 41 = 41.$
  $2^2 - 2 + 41 = 43.$
  $3^2 - 3 + 41 = 47.$
  $4^2 - 4 + 41 = 53.$
  $5^2 - 5 + 41 = 61.$

- Is this a theorem? It seems that you would always get a prime number—no matter what number you plug in. However, in 1772, Euler noted that you always get a prime number up to 40, but at 41, the answer is no longer a prime number: $41^2 - 41 + 41 = 41^2$, which is not a prime number because it has been factored into 41×41.

- You can't prove a theorem by doing a lot of examples. In this case, 40 examples always give a prime number, but it still isn't a theorem.

Examples of False Conjectures

- To prove that any conjecture or equation is false, all you have to do is find a single counterexample.

- Assuming that a and b are positive, does $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$? Is this always true? No, it's not true; there are many counterexamples. If a and b are both equal to 1, then the right-hand side of the equation is $\sqrt{1} + \sqrt{1} = 1 + 1 = 2,$ and the left-hand side is $\sqrt{2}$, which doesn't equal 2. That's an irrational number, in fact. Note that for positive real numbers, the following is true: $\sqrt{ab} = \sqrt{a}\sqrt{b}.$

- Is it always true that $\frac{1}{x+y} = \frac{1}{x} + \frac{1}{y}$? A counterexample is if x and y both equal 1. Note that you can split up numerators, but you can't split up denominators. In fact, it is true that $\frac{x+y}{z} = \frac{x}{z} + \frac{y}{z}.$

- Does $\sin(2x) = 2\sin(x)$? For people who have studied trigonometry, this is a common mistake. If $x = \pi/2$, then $2 \times (\pi/2) = \pi$ and $\sin(\pi) = 0$. However, $2\sin(\pi/2) = 2 \times 1 = 2$. Therefore, when $x = (\pi/2)$, the left-hand side equals 0, and the right-hand side equals 2.

- Does $\log(x + y) = \log(x) + \log(y)$? For this example, it doesn't matter whether you use logarithms with base 10 or base e. This is an incorrect usage of logarithms. If you're using logarithms with base 10, then let x and y both equal 10, which means that both logarithms on the right-hand side of the equation are equal to 1 because $\log(10) = 1$. However, $\log(10 + 10) = \log(20) \approx 1.301$. Note that it is true that $\log(xy) = \log(x) + \log(y)$.

- In calculus, the derivative of the sum of 2 functions equals the sum of their derivatives—but this is not true for the derivative of the product of 2 functions. In fact, the derivative of a product is a more complicated formula. To prove that the derivative of a product is not the product of the derivative, you would find a counterexample.

Fermat's Conjecture

- In 1640, Fermat conjectured that the numbers of the form $F_n = 2^{2^n} + 1$ were always going to be primes (for all $n = 0, 1, 2, 3, \ldots$). Those numbers are called Fermat numbers. As a review, $2^{2^n} = 2^{(2^n)}$. It is not equal to $\left(2^2\right)^n$.

- To begin to analyze this conjecture, compute the first few Fermat numbers.

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3.$$

$$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5.$$

$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17.$$

$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257.$$

$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65{,}536 + 1 = 65{,}537.$$

- Note that all of these numbers are prime numbers. Fermat's conjecture is that they will continue to be primes.

- Almost 100 years later, Euler showed that Fermat's conjecture was wrong. He found a counterexample. He computed the next number in the list, F_5: 4,294,967,297. Euler was able to factor that into its 2 prime factors: 641 × 6,700,417. Today's calculators can easily factor that number and produce those 2 prime factors.

- Fermat's conjecture is wrong, but it gave birth to a new conjecture: None of the rest of the numbers—F_6, F_7, and so on—are primes; instead, they are all composite numbers. This is unproven to this day.

- It's amazing that Euler and Fermat were able to do these computations without computers. Today, computers play a large role in mathematics.

Mathematical Paradoxes

- The following is a paradox of language: "This statement is false." Think about that sentence. There has been a lot of history and philosophical discussion about it. Explore this paradox at your leisure.

- The following paradox from set theory is a paradox that Galileo observed: 2 sets have the same cardinality, yet one is a proper subset of the other. In other words, you can have 2 sets in which one is a subset of the other, yet they have the same number of elements in the sense that you can match up the elements of one set with all the elements of the other set.

- Galileo observed that there are as many square numbers as there are positive integers. That paradox has been answered—now that mathematicians have understood more about infinite sets and about cardinality of infinite sets.

- Then, there are the famous paradoxes of Zeno, which are very old and generally deal with infinite sums. One of Zeno's paradoxes can be simplified into the following: Suppose that you want to walk 1 mile. First, you have to walk 1/2 of a mile. Then, you have to walk 1/4 of a mile. Then, you have to walk 1/8 of a mile. Then, you walk 1/16 of a mile. The paradox is that you never reach the end.

- Mathematicians have answered that paradox through their study of infinite geometric series. Think of this paradox as involving the summation of $1/2 + 1/4 + 1/8 + 1/16 + \ldots$. The sum of that geometric series equals 1, so you actually do reach 1 mile.

- Perhaps the most important and famous paradox in all of mathematics is Russell's paradox, which is named after Bertrand Russell. It's actually a set theory paradox, but it can be described in many different ways.

- Imagine that a town has a barber, and the barber follows the following rule: He only cuts the hair of those people who do not cut their own hair. Who cuts the barber's hair? There are 2 possible answers: The barber could cut his hair, or he might not. Analyze each in turn.

- If the barber does not cut his own hair, then he should because he cuts the hair for all the people who do not cut their own hair. If the barber does cut his own hair, then he breaks the rule that he only cuts the hair of people who do not cut their own hair. This is a real paradox.

- Historically, this was a paradox that shook the foundations of set theory. Bertrand Russell developed this paradox in around 1901 and showed that the set theory that had been developed by Cantor and other mathematicians can have contradictions if it's not done correctly.

- When dealing with set theory, you have to be careful with the idea that a set might contain itself as a member. This is very deep mathematics; it's something that most students would study in a graduate course on logic and set theory.

PROBLEMS

1. Prove or disprove the following conjecture: If $n > 1$ is prime, then $2^n - 1$ is also prime.

2. Prove or disprove the following conjecture: There exists a real number x such that $x^4 + 2x^2 + 1 = 0$.

When 1 = 2—False Proofs

Lecture 18

In this lecture, you will learn about false proofs, or proofs of theorems that have errors in them—errors that are often very subtle. Hopefully, looking at false proofs will strengthen your knowledge of good proof techniques. Throughout the lecture, you will be exposed to some common errors in writing proofs. In addition, you will encounter some classic problems that have been proven to be impossible to do, despite the fact that many people are still trying to do them.

False Proofs

- There is a famous proof that states that 2 = 1. There are many proofs that are similar to this one, and they appear in many textbooks on proof theory. Of course, it's not true that 2 = 1, so your challenge is to find the mistake in the following proof.

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

- Probably the most obvious mistake is in the line where $x - y$ is on both sides of the equation and are cancelled. The proof started with $x = y$ (and, therefore, $x - y = 0$), and you can't divide an equation by 0. Dividing by 0 is a very common trick to generate proofs like this.

- Another false proof involves proving that 0 = 1. Again, it's not true.

$$0=0+0+0+\ldots$$
$$0=(1-1)+(1-1)+(1-1)+\ldots$$
$$0=1+(-1+1)+(-1+1)+(-1+1)+\ldots$$
$$0=1+0+0+\ldots$$
$$0=1.$$

- The mistake is in the second line: $0 = (1 - 1) + (1 - 1) + (1 - 1) + \ldots$. That infinite series does not converge, so you can't manipulate it in that way. This is the subject of second-semester calculus. It's a very subtle error, and when one studies infinite series, this problem often occurs.

- Another common error in writing proofs is to begin with what you want to prove. If you want to prove a theorem, you're supposed to start with a hypothesis, do some math, and end up with a conclusion. If you start with the conclusion, do some math, and end up with a true statement, then you might think that, because you ended up with a true statement, the beginning part of your proof is also true.

- For example, prove that for all x, $x - 2 = 2 - x$. Find a counterexample: Let x be 0, and you will quickly see that this is not a true theorem. Starting with the conclusion, the "proof" is as follows.

$$\begin{aligned} x-2 &= 2-x \\ (x-2)^2 &= (2-x)^2 \\ x^2-4x+4 &= 4-4x+x^2 \\ 4 &= 4. \end{aligned}$$

- Does the fact that you ended up with a true equation mean that what you started with is also true? No, it doesn't. Just because you can start at the top and go to the bottom of the proof doesn't mean that you can start with 4 = 4, a true statement, and get back to the beginning. In fact, when you start squaring numbers—or taking square roots of numbers—you can introduce some false proofs in which it would be impossible to go backward.

- However, it often helps to play around with what you want to prove because it might yield the proof or it might give you an idea of what the proof is. On scratch paper, you can play with the conclusion and then possibly determine what the proof should be, but then, throw your scratch paper away and write the proof.

- Another example of that technique is as follows. The theorem that you want to prove is that for any real number x, $x^2 - 2x + 2 > 0$. To prove this, start by trying some examples. If you plug in some x values, you will see that the expression is always positive. However, just because you found a few values of x that made it positive, it doesn't mean that every value of x makes it positive. Doing examples is not a proof; it just gives you confidence that what you are trying to prove is probably true.

- To prove it, use some scratch paper to start playing with the conclusion, hoping that it will generate some ideas about how the proof should go.

$$\begin{aligned} x^2 - 2x + 2 &> 0 \\ x^2 - 2x + 1 + 1 &> 0 \\ (x-1)^2 + 1 &> 0. \end{aligned}$$

- The ultimate inequality, $(x - 1)^2 + 1 > 0$, is a true statement because $(x - 1)^2$ is nonnegative (any real number squared is greater than or equal to 0) and you are adding 1 to that nonnegative number. Therefore, the left-hand side is bigger than 0. Because you now see how the proof is going to go, you can reverse your steps.

$$\begin{aligned} (x-1)^2 + 1 &> 0 \\ x^2 - 2x + 1 + 1 &> 0 \\ x^2 - 2x + 2 &> 0. \end{aligned}$$

- Without scratch paper, it might have been very difficult to come up with that proof. However, the scratch paper was not the proof. Mathematicians typically use scratch paper when doing proofs.

Impossible Euclidian Geometry

- Historically, there are many conjectures and theorems that have had false proofs published. For example, the 4-color theorem had some false proofs published well before it was finally established.

- There are also the classic ruler-and-compass constructions from ancient Greek mathematics, or Euclidian geometry. These are constructions in which you are allowed to use an unmarked straightedge and a compass.

- There are 3 classic ruler-and-compass constructions that are impossible to do. The first one involves trisecting an angle. You know how to bisect an angle with a ruler and compass, but given an arbitrary angle, is it possible to trisect it? In other words, is it possible to find 2 rays coming out of the vertex such that all 3 angles have the same measure? It turns out that trisecting an angle has been proven impossible by Galois theory, which is studied in postgraduate mathematics courses.

- The second classic problem involves duplicating a cube. Given a cube of side length s, can you construct—with a ruler and compass—a cube having twice the volume of the original cube? This is impossible, and it has been proven to be impossible.

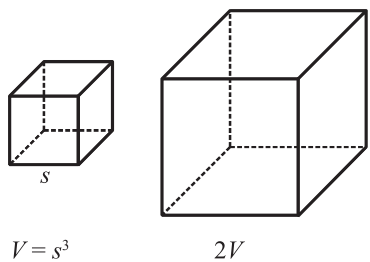


Figure 18.1

- The third classic problem involves squaring a circle. Can you construct a square with the same area as a given circle? This is also impossible. In this case, the impossibility is based on the subtle fact that π is a transcendental number; in other words, π is not the root of any polynomial equation having integer coefficients.

Fermat's Last Theorem

- One of the most famous theorems of all time in mathematics is Fermat's last theorem. Recall that the Pythagorean theorem, $a^2 + b^2 = c^2$, is true for right triangles, where a and b are the measures of the sides and c is the hypotenuse. For example, the 3-4-5 right triangle satisfies the Pythagorean theorem.

- If you change the exponent from 2 to a higher integer—such as 3, 4, 5, or any positive integer n—then Fermat's last theorem states that there are no positive integer solutions: $a^n + b^n = c^n$, $n > 2$.

- This theorem was conjectured in 1637 by Pierre de Fermat, who is said to have written the conjecture as a marginal note in a book but didn't have enough room to write down the proof. For many years, mathematicians have tried to prove this theorem, and there have been thousands of false proofs submitted.

- Finally, Fermat's last theorem was proven by Andrew Wiles, who supposedly dedicated 7 years to trying to prove it. He built his proof on the results of others. It turns out that there was a slight mistake in his work, and it took a few extra years to correct it, but mathematicians today accept Wiles's proof that Fermat's last theorem is true.

Euclid's Fifth Postulate

- Another area of mathematics in which many false proofs were published is in the area of Euclidian geometry—specifically in regard to the parallel postulate.

- Recall that Euclid had 5 postulates, and his fifth postulate was pretty complicated. Euclid's fifth postulate is equivalent to the following parallel postulate: Given a point P not on a line l, there exists exactly 1 line through P parallel to l.

- This postulate seems so self-evident that as soon as Euclid's *Elements* was published—and for about 2000 years after—people began to try to prove the fifth postulate from the previous 4 postulates. Many false proofs were published.

- Then, it was discovered that the fifth postulate was not a theorem but, rather, an axiom that was independent of Euclid's other axioms. This discovery gave rise to non-Euclidian geometry, where there is, in fact, more than 1 parallel line through the point P to the line l.

A False Proof from Mathematical Induction

- A well-known false proof from mathematical induction involves the following statement: All horses have the same color. While you probably do not believe that the statement is true, prove that all horses have the same color by mathematical induction.

- First, consider the base case; consider that a single horse has the same color as itself. For example, use the color gray. Then, assume that this is true for n horses; assume that they all have the same color (gray). That's the induction hypothesis. You want to prove that a group of $n + 1$ horses all have the same color.

- Consider a group of $n + 1$ horses, and take off the first n. By the induction hypothesis, they all have the same color because there are n of them and they are all gray. Next, take a different group of n horses and look at horse number 2, 3, 4, …, $n + 1$. By the induction hypothesis, that group of n horses also has the same color, which is gray because horse number 2 is in both groups.

- Where's the flaw? If you look closely, this proof breaks down in the case where $n = 1$—in other words, when you have just $n = 1$ and $n + 1 = 2$. The induction step does not work if $n = 1$. This theorem is false.

- Instead of horses, use numbers: All numbers are equal to each other. Prove this theorem by mathematical induction. This theorem is true for a single number, the base case, because a single number is equal to itself. Assume that it's true for n numbers, $x_1, x_2, \ldots, x_n$. If you have n numbers, then they are all equal to each other by the induction hypothesis.

- Consider a set of $n + 1$ numbers: $y_1, y_2, \ldots, y_n, y_{n+1}$. You want to show that all of these numbers are equal to each other. The first n of these numbers are, indeed, equal to each other by the induction hypothesis. The last n numbers—$y_2, \ldots, y_{n+1}$—are a set of n numbers and are all equal to each other by the induction hypothesis. In fact, y_2 is in both sets, so every number is equal to y_2, and all the numbers are equal to each other.

- Where's the flaw? This proof doesn't work if you have $n = 1$ and then $n + 1 = 2$.

PROBLEMS

1. Find the mistake in the following argument that 0 = 1.

$$\begin{aligned} x &= 0 \\ x(x-1) &= 0 \\ x-1 &= 0 \\ x &= 1 \\ 0 &= 1. \end{aligned}$$

2. Comment on the proof of the following "theorem": For all real numbers $x,\ 2x^2 - 8 = 0$.

$$\begin{aligned} 2x^2 - 8 &= 0 \\ x^2 - 4 &= 4 - x^2 \\ \left(x^2 - 4\right)^2 &= \left(4 - x^2\right)^2 \\ x^4 - 8x^2 + 16 &= x^4 - 8x^2 + 16 \\ 16 &= 16. \end{aligned}$$

A Picture Says It All—Visual Proofs

Lecture 19

In this lecture, you will learn that a mathematical statement or theorem can be visualized. With visual proofs, you confirm your belief in a statement or theorem by seeing a picture. However, because they are not written as logical arguments, visual proofs are not always considered to be analytic proofs. In this lecture, you will be introduced to examples of visual proofs, and you will revisit some theorems that you have proven with other techniques.

Visually Proving the Pythagorean Theorem

- The validity of a mathematical statement can often be established by an appropriate diagram or picture. These are called visual proofs, or proofs without words.

- There are hundreds, if not thousands, of proofs of the Pythagorean theorem: $a^2 + b^2 = c^2$ for right triangles, where c is the hypotenuse and a and b are the legs. Perhaps the simplest example is the 3-4-5 right triangle, which has legs of size 3 and 4 and a hypotenuse of size 5: $3^2 + 4^2 = 5^2$.

- To construct a visual proof of the Pythagorean theorem, form 2 squares with sides of length $a + b$. In other words, each square is $a + b$ by $a + b$. Hence, they have the same area: $(a + b)^2$.

- Divide the 2 squares in the following way.

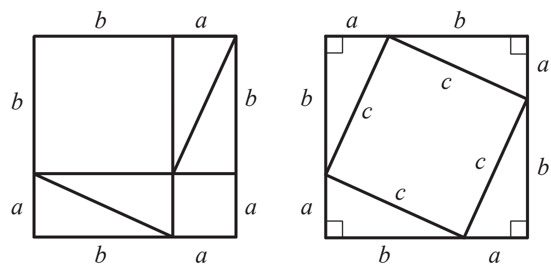


Figure 19.1

- Left square = $a^2 + b^2 + 4\left(\frac{1}{2}ab\right) = a^2 + b^2 + 2ab.$
- Right square = $c^2 + 4\left(\frac{1}{2}ab\right) = c^2 + 2ab.$
- If you set the 2 equations equal to each other, $a^2 + b^2 + 2ab = c^2 + 2ab$, you are left with the Pythagorean theorem: $a^2 + b^2 = c^2$.

President Garfield's Proof

- President Garfield once published an original proof of the famous Pythagorean theorem. In 1876, before he became the 20th president of the United States, he developed a proof of the theorem using trapezoids.

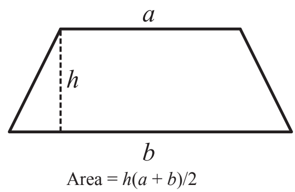


Figure 19.2

- Recall from geometry that a trapezoid has 2 parallel sides, a and b, and that the height of a trapezoid is the distance between those 2 parallel sides. The formula for the area of a trapezoid is $h(a + b)/2$. You can think of that as follows: The height is h, and then $a + b$ divided by 2 is the average of the lengths of the 2 parallel sides.

- President Garfield constructed a trapezoid in the following way.

- He calculated the area of the large trapezoid in 2 different ways.

$$\frac{1}{2}h(a+b) = \frac{1}{2}(a+b)(a+b).$$

$$2\left(\frac{1}{2}ab\right) + \frac{1}{2}c^2.$$

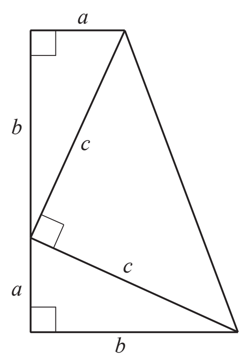


Figure 19.3

- He then set those 2 terms equal to each other and proved the Pythagorean theorem results.

$$\frac{1}{2}(a+b)(a+b) = 2\left(\frac{1}{2}ab\right) + \frac{1}{2}c^2$$

$$(a+b)(a+b) = 2(ab) + c^2$$

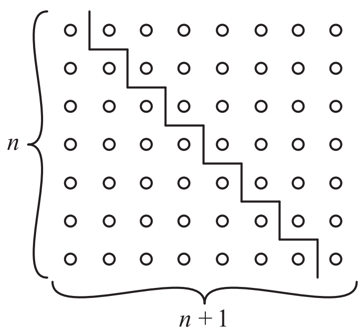
$$a^2 + 2ab + b^2 = 2ab + c^2$$

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

Summation

- A theorem that has been presented many times in these lectures is the sum of the first n positive integers: $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$. This theorem has many proofs, including direct proofs and mathematical induction proofs.

- To construct a visual argument for this theorem, consider an array of dots of size n by $n + 1$. The total number of dots is $n(n + 1)$.



Total dots: $n(n+1) = [1+2+\dots+n]+[1+2+\dots+n]$

Figure 19.4

- If you count the dots to the left-hand side of the diagonal line, the sum is $1 + 2 + \dots + n$. If you count the dots on the right-hand side of the diagonal, the sum is $1 + 2 + \dots + n$.

- Therefore, $(1 + 2 + \ldots + n) + (1 + 2 + \ldots + n) = n(n + 1)$.

$$2(1 + 2 + \ldots + n) = n(n + 1)$$
$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

- Another summation problem (proved by mathematical induction) that appeared in a previous lecture is $1 + 3 + \ldots + (2n - 1) = n^2$.

- To construct a visual proof, consider an array of n by n dots. The total number of dots in the array is n^2. Count the dots in the figure, starting in the bottom left and working your way to the upper right: $1 + 3 + 5 + 7 + \ldots$. This equals the total number of dots, n^2.

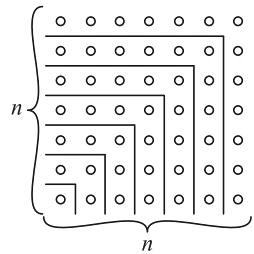


Figure 19.5

Geometric Series

- Recall the geometric series $1 + 1/2 + 1/4 + 1/8 + \ldots = 2$. If you subtract 1 from both sides, you get a very similar formula: $1/2 + 1/4 + 1/8 + \ldots = 1$. This might remind you of Zeno's paradox.

- To construct a visual proof of this formula, consider a square that is 1×1, so the area of that square is 1. Divide it vertically down the middle, and on the left-hand side, you have a rectangle of area 1/2. Divide the right-hand side horizontally, and the bottom part now has an area of 1/4. Divide the upper-right square vertically, and the left-hand rectangle in that upper-right square has an area of 1/8. If you keep dividing, you approach the upper-right corner. If you divide infinitely, you get the series $1/2 + 1/4 + 1/8 + \ldots$, and it fills out the entire square whose area is 1.

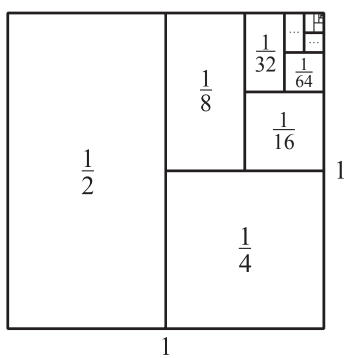


Figure 19.6

Set Theory

- You can use Venn diagrams to verify set theory properties, such as the distributive property: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. In this equation, *A*, *B*, and *C* are all subsets of some universal set. If you take the union of *B* and *C* and intersect that with *A*, that would be the same as intersecting *A* with *B*—and also intersecting *A* with *C*—and then taking their union.

- You can visually verify the distributive property for set theory by drawing the Venn diagram for each side of the equation. You will see that the Venn diagram is the same for both sides, so it is probably a true equation.

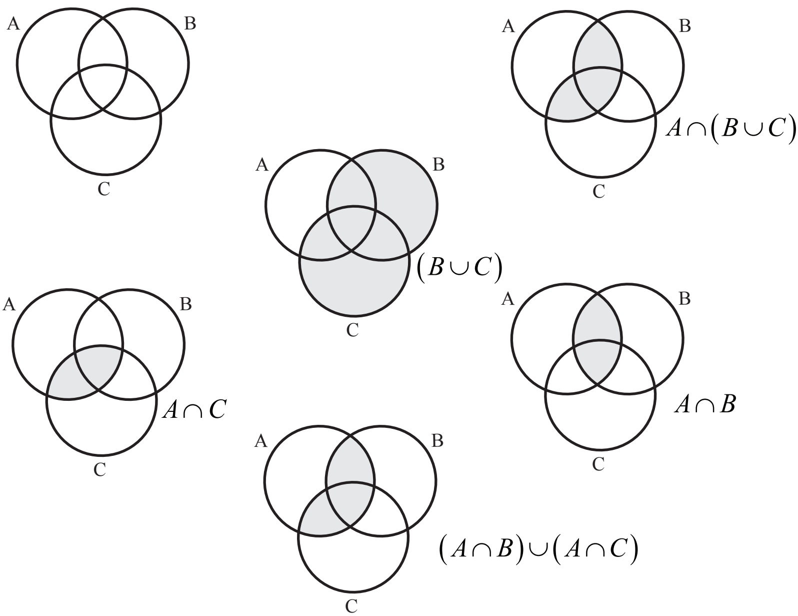


Figure 19.7

The Arithmetic-Geometric Mean Inequality

- Let a and b be 2 positive real numbers. The arithmetic mean is their average: $\frac{a+b}{2}$. The geometric mean of 2 numbers is the square root of their product: $\sqrt{ab}$.

- To determine if there is a relationship between these 2 means, try some examples and then try to prove the theorem.

$$a = 2, b = 8: \frac{1}{2}(a+b) = 5;\ \sqrt{ab} = \sqrt{16} = 4.$$

$$a = 7, b = 5: \frac{1}{2}(a+b) = 6;\ \sqrt{ab} = \sqrt{35} \approx 5.9.$$

$$a = 11, b = 11: \frac{1}{2}(a+b) = 11;\ \sqrt{ab} = 11.$$

- The conjecture is that the arithmetic mean is less than or equal to the geometric mean. In fact, you could add that there is equality when the numbers are the same. Therefore, for a and b, which are positive real numbers, $\frac{1}{2}(a+b) \geq \sqrt{ab}$. In addition, there is equality when $a = b$.

- Construct a visual proof. Without loss of generality, assume that $a > b$. Construct a square of sides $a + b$ by $a + b$. The total area of the square is $(a + b)(a + b)$. This equals the sum of the 4 rectangles and the area of the small square in the center of the following figure.

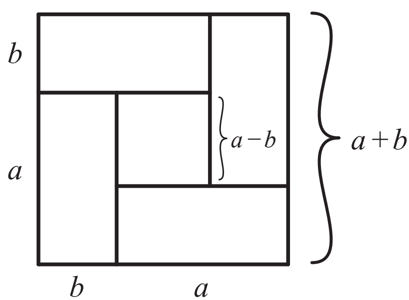


Figure 19.8

$$(a+b)^2 = 4ab + (a-b)^2$$
$$(a+b)^2 \geq 4ab$$
$$a+b \geq \sqrt{4ab} = 2\sqrt{ab}$$
$$\frac{1}{2}(a+b) \geq \sqrt{ab}.$$

- To prove the formula analytically, without a picture, do a direct proof. You want to prove that $\frac{1}{2}(a+b) \geq \sqrt{ab}$. Using some scratch paper, start by manipulating the conclusion.

$$\frac{1}{2}(a+b) \geq \sqrt{ab}$$
$$a+b \geq 2\sqrt{ab}$$
$$a^2 + 2ab + b^2 \geq 4ab$$
$$a^2 - 2ab + b^2 \geq 0$$
$$(a-b)^2 \geq 0.$$

- The statement $(a - b)^2 \geq 0$ is always true; the square of any real number is nonnegative.

- Next, you should be able to construct your proof using the work you did on scratch paper. Start with the last line of your work and go backward.

$$(a-b)^2 \geq 0$$
$$a^2 - 2ab + b^2 \geq 0$$
$$a^2 + 2ab + b^2 \geq 4ab$$
$$(a+b)^2 \geq 4ab$$
$$a+b \geq 2\sqrt{ab}$$
$$\frac{1}{2}(a+b) \geq \sqrt{ab}.$$

- Notice that if $a = b$, then there is equality in the equation.

$$\frac{1}{2}(a+b) = \frac{1}{2}(2a) = a$$

$$\sqrt{ab} = \sqrt{a^2} = a.$$

Another Summation Example

- To construct another visual proof of the theorem for the sum of the first n positive integers—$1 + 2 + \ldots + n = n(n+1)/2$—form a right triangle of blocks that are n by n. The sum of the areas of all of the blocks is $1 + 2 + \ldots + n$. The sum is also equal to the area of the triangle plus the area of the shaded part: $n^2/2 + n/2 = \dfrac{n(n+1)}{2}$. Then, that equals $1 + 2 + \ldots + n$.

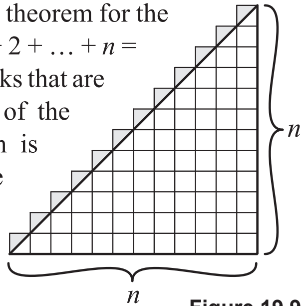


Figure 19.9

PROBLEMS

1. Show by way of an appropriate counterexample that the following set theory conjecture is false.

$$A \cap (B \cup C) = (A \cap B) \cup C.$$

2. What is the sum of the first 100 odd natural numbers? What is the sum of the first 100 even natural numbers?

The Queen of Mathematics—Number Theory

Lecture 20

Number theory is considered the heart of pure mathematics. This lecture focuses on prime numbers, but number theory is a much broader field that encompasses many other topics. Specifically, you will learn about the sieve of Eratosthenes, which can be used to generate prime numbers up to a certain number *n*. In addition, you will learn that factoring integers into primes is theoretically possible but, in practice, can be very difficult. Furthermore, you will be exposed to Euclid's beautiful proof that there are an infinite number of primes.

Number Theory

- Number theory is one of the oldest parts of mathematics. On one level, it's the study of the natural numbers (1, 2, 3, …), but it's really the study of all numbers. It includes such topics as prime numbers, factorization, division, properties, and more.

- The formal definition of a prime number is a positive integer greater than 1 is a prime number if its only divisors are 1 and itself. In particular, 1 is not a prime number; 2 is the first prime number.

- You can divide the positive integers into prime numbers and composite numbers. For example, 2, 3, 5, and 7 are prime numbers, but 8, 9, and 15 are composite numbers because they have other divisors.

- One way to tell if a positive integer is prime is to try to factor it. However, that can be quite difficult. Factoring is one of the most difficult algorithms for computers to solve.

- Perhaps the easiest way—and one of the most efficient ways—to make a list of prime numbers is by using a technique called the sieve of Eratosthenes. Around 200 B.C., Eratosthenes was the director of the library in Alexandria, Egypt.

- Suppose that you want to find all of the prime numbers that are less than 100. Write down all of the natural numbers from 2 to 100 (you do not have to include 1 because 1 is not a prime number). In the first row, write 2 through 10, and in the second row, write 11 through 20, and so on. The final row is 91 through 100.

- Start with 2, the first prime number. Circle it. Then, cross out all multiples of 2 up to 100. All of those numbers that you cross out aren't primes because they have 2 as a factor. Then, circle the next prime number, 3, and cross out all the multiples of 3 up to 100. Continue with 5 and 7.

- You can stop at 7 without having to worry about 11, 13, or other primes because if there were a composite number left in the chart that wasn't crossed off yet, then 2, 3, 5, and 7 would not be one of its prime factors because every number that has a prime factor of 2, 3, 5, or 7 has been crossed off. Therefore, it must have a prime factor of 11 or even larger. If one of its prime factors is 11—or greater than 11—then its other prime factor will be smaller than 11, such as 7, but that's impossible.

- If you want to find the prime numbers up to 100, then you just have to do the sieve up to $\sqrt{100}$. In other words, use the prime number right before $\sqrt{100}$ as your ending point. For example, the $\sqrt{100}=10$, so you know that you can stop this process at the prime number 7, which is the closest prime number to 10 without going above 10.

- After crossing off all of the composite numbers, you are left with 25 prime numbers between 2 and 100: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97. There are no other prime numbers between 2 and 100.

- Prime numbers are the building blocks of the integers. Recall the fundamental theorem of arithmetic: Every integer greater than 1 can be uniquely written as a product of primes (up to order). This is an existence and uniqueness theorem, the existence part of this theorem was proven in a previous lecture.

- Given a positive integer, you can break it down into its prime factors. For example, $66 = 2 \times 33 = 2 \times 3 \times 11$.

- Is it practical to take a large positive integer and find its prime factors? Modern graphing calculators can factor positive integers of about 50 or 100 digits, depending on the number.

- Suppose that you have a number of 500 digits—a giant integer. Suppose that it only has 2 prime factors and that each of those factors is huge. It would take a very long time for the world's fastest computer to factor that composite number into its 2 factors. The difficulty of factoring large integers into their prime factors is the basis of many algorithms of modern cryptography.

Euclid's Proof by Contradiction

- In *Elements*, Euclid claimed that there are an infinite number of prime numbers. To prove this, do a proof by contradiction. Assume, by way of contradiction, that there's a finite number of primes.

- Euclid said that in order to prove that there are an infinite number of primes, assume, by way of contradiction, that there is a finite set of primes: $P = \{p_1, p_2, \ldots, p_n\}$.

- To get a contradiction with this supposition, Euclid constructed a new number, m, that is equal to the product of the n primes plus 1: $m = (p_1 \times p_2 \ldots p_n + 1)$.

- Is m divisible by any of the prime numbers p_1 through p_n? No, because every time you divide one of the known primes into m, you get a remainder of 1. Therefore, m is not divisible by any of the known primes. Furthermore, if m has no prime divisors, then either it must be prime or it is divisible by a prime that is not on the list. In either case, that is the contradiction.

- Euclid assumed that there were a finite number of primes, constructed the new number m, and then discovered the contradiction that either m is prime or m has prime factors that are not on the list.

- Illustrate the proof with a few numerical examples. Suppose that the list of prime numbers only contained 4 numbers—2, 3, 5, and 7—and that there are no more prime numbers. How would the theorem derive a contradiction? You would form m, which is 2(3)(5)(7) + 1. That equals 211, which is a prime number. That is a contradiction because 211 is not in the list of the 4 primes.

- Suppose that the list of primes was slightly larger—2, 3, 5, 7, 11, and 13, for example. If that were the list of all the prime numbers in the world, then you could find m by multiplying those numbers together and adding 1: 2(3)(5)(7)(11)(13) + 1. That equals 30,031, which is not prime, but it has prime factors that are larger than 13. Its prime factors are 59 and 509, and that is the contradiction.

- This is an elegant proof by contradiction. It is done in many math courses, and probably every mathematician in the world knows this proof.

The Twin Prime Conjecture

- The twin prime conjecture is unsolved to this day. If you look at a list of primes, you will see that some of them differ just by 2 units—for example, 5 and 7 or 11 and 13. These are called twin primes.

- You can start writing down examples of twin primes, such as 5 and 7, 11 and 13, 29 and 31, and so on. How many twin primes are there? Are there an infinite number of twin primes? This is unknown to this day. People have made progress on how to study this problem by using computers, but it is still unsolved.

PROBLEMS

1. Factor the integers 30,030 and 1537. Which was easier to do?

2. Use the sieve of Eratosthenes to find all the prime numbers between 100 and 200. How many are there?

Primal Studies—More Number Theory
Lecture 21

In this second lecture on number theory, you are going to be exposed to more theorems about prime numbers. In particular, you will learn about the distribution of prime numbers—how they thin out as *n* increases. In addition, you will be introduced to an interesting proof that uses factorials to show that there are arbitrarily large prime gaps. You will also be presented with more unsolved problems in mathematics; these problems are easy to state but difficult to solve.

The Distribution of Prime Numbers

- Euclid proved that there are an infinite number of primes, but how are the primes distributed? You can begin to answer that by forming a table.

- What do you observe? The number of primes seems to thin out; there are fewer primes in each of the collections of numbers. Are there any patterns to this thinning?

Table 21.1

Number Scale	Number of Primes
1−1000	168
1001−2000	135
2001−3000	127
3001−4000	120

- For every positive integer n, there is a sequence of n consecutive positive integers containing no prime numbers (in other words, composite numbers).

- For example, if $n = 3$, 3 consecutive composites are 8, 9, and 10 or 14, 15, and 16. If you can find 3 consecutive composite numbers, they are said to have a prime gap of length 3. Furthermore, if $n = 5$, there is a prime gap of 5: 32, 33, 34, 35, and 36.

- The proof of this theorem involves factorials. Recall that 2! is 2×1, or 2, and 3! is $3 \times 2 \times 1$, or 6. Notice that the divisors of 4!—which is $4 \times 3 \times 2 \times 1 = 24$—include 4, 3, 2, and 1.

- In the case where $n = 4$, you can construct a sequence of 4 consecutive composite numbers: $5! + 2 = 122$, $5! + 3 = 123$, $5! + 4 = 124$, and $5! + 5 = 125$. These 4 consecutive numbers—122, 123, 124, and 125—are all composite. For example, 122 is made up of $5! + 2$, and 2 is a factor of that number because $5! = 5 \times 4 \times 3 \times 2$. In other words, 122 is divisible by 2, 123 is divisible by 3, 124 is divisible by 4, and 125 is divisible by 5. This is a proof by construction.

- For the general proof, let n be given. You want a string of n consecutive composite numbers. Consider $(n + 1)! + 2$, $(n + 1)! + 3$, $+ \ldots + (n + 1)! + (n + 1)$. This is a list of n numbers. The first one is divisible by 2—because it's $(n + 1)! + 2$—so it's composite. The second one is divisible by 3, so it's composite. The n^{th} number is divisible by $(n + 1)$, so it's composite as well.

- This is a proof by construction. Given n, you can construct a list of n consecutive composite numbers.

The Prime Counting Function

- How many prime numbers are there up to a given number n? Mathematicians have defined a function in order to analyze this question. The prime counting function $\pi(n)$ is the number of primes less than or equal to n. For example, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(4) = 2$, $\pi(10) = 4$, $\pi(100) = 25$, and $\pi(1000) = 168$.

- What is the behavior of this function? As n grows, so does $\pi(n)$. Clearly, it's increasing, but how fast? The prime number theorem relates $\pi(n)$, the number of primes $\leq n$, to the natural logarithm function. It describes the distribution of prime numbers. Some of the greatest mathematicians have worked on this problem, including Legendre, Gauss, Chebyshev, and Riemann.

- Logarithms are generally studied in algebra or precalculus courses. In those courses, you might have seen logarithms to base 10, but in calculus, you use base e, where e is approximately 2.718. Both logarithms and exponentials (e^x) are built into calculators. For the purposes of this course, you only need to know how to calculate logarithms with a calculator.

- If you have a calculator, you can verify the following logarithms.

  $\ln(1) = 0.$

  $\ln(10) \approx 2.30.$

  $\ln(100) \approx 4.61.$

  $\ln(1000) \approx 6.91.$

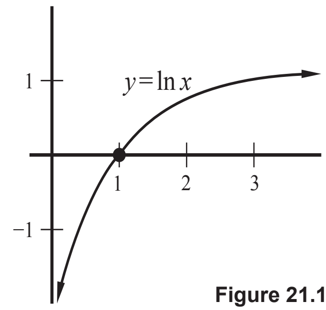


Figure 21.1

- When you use your calculator, make sure you use base e and not base 10. Calculators usually have both keys. You may be surprised to learn that the logarithm function grows slowly.

- The prime number theorem states that the ratio of $\pi(n)$ and $n/\ln(n)$ approaches 1 as n grows without bound—as it extends to infinity. Mathematicians say that $\pi(n)$ and $n/\ln(n)$ are asymptotic because their ratio approaches 1.

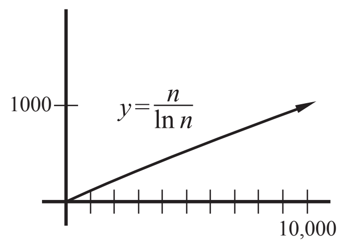


Figure 21.2

Table 21.2

n	$\pi(n)$	$n/\ln n$	ratio
10^3	168	144.8	1.161
10^6	78,498	72,382.4	1.084
10^9	50,847,534	48,254,942.4	1.054

- According to unpublished papers, Gauss seemed to have known this result in 1793, but it was finally proven—officially and independently—by 2 mathematicians, Jacques Hadamard and C. J. de la Vallee-Poussin, in 1896.

- It turns out that there are even better approximations available for the number of primes that are less than or equal to n. Many of them involve integrals, which require a knowledge of calculus.

Unsolved Problems

- The famous twin prime conjecture states that there are infinitely many twin primes. Recall that twin primes are 2 prime numbers that differ by 2 units. For example, 3 and 5 or 5 and 7. Euclid proved that there are infinitely many primes, but are their infinitely many twin primes?

- Evidence seems to support the twin prime conjecture. Mathematicians have used computers to find many twin primes that are huge numbers; as a result, they conjecture that there are an infinite number of them. It would be difficult to prove that the list stops. For example, 1,000,000,000,061 and 1,000,000,000,063 are twin primes.

- Another great unsolved problem is the Goldbach conjecture, which claims that every even integer greater than 2 can be expressed as the sum of 2 primes. For example, $8 = 3 + 5$ and $14 = 3 + 11 = 7 + 7$. If you try more examples, you will see that this seems to always be true.

- The German mathematician Christian Goldbach first posed this problem in a letter to Euler in 1742. Euler couldn't prove it, and in fact, nobody has been able to prove it to this day. There are many partial results and many computer studies.

- The Collatz problem was first proposed by Lothar Collatz in 1937. It is also known as the $3n + 1$ conjecture or the Ulam conjecture (named after the mathematician Stan Ulam).

- Take any positive integer n. If it's even, divide it by 2; if it's odd, multiply it by 3 and then add 1. For example, 5 is odd, so multiply it by 3 and add 1: $5 \times 3 = 15 + 1 = 16$. Because 16 is even, divide it by 2 to get 8, which is even. Divide 8 by 2 to get 4, which is even. Divide 4 by 2 to get 2, which is even. Finally, divide 2 by 2 to get 1.

- You might observe that no matter what number you select, the sequence will ultimately reach 1. Nobody has ever proven this conjecture.

- Finally, there are some problems that involve perfect numbers that remain unsolved to this day. In order to define the concept of a perfect number, begin with the proper divisors of integers.

- For example, what are the proper divisors of 4? In other words, what numbers divide into 4 evenly? The only divisors—other than 4—that evenly divide into 4 are the numbers 1 and 2. In addition, the only proper divisor of 5 is 1. The proper divisors of 6 are 1, 2, and 3. The proper divisors of 8 are 1, 2, and 4. Finally, the proper divisors of 12 are 1, 2, 3, 4, and 6.

- Knowing how to find the proper divisors, add them for a given integer as follows.

  4: $1 + 2 = 3$.
  5: $1 = 1$.
  6: $1 + 2 + 3 = 6$.
  8: $1 + 2 + 4 = 7$.
  12: $1 + 2 + 3 + 4 + 6 = 16$.

- Note that 6 equals the sum of its proper divisors. That's a perfect number. A positive integer is a perfect number if it equals the sum of its proper divisors.

- Are prime numbers perfect? No, because remember that the only proper divisor for 5 is 1, which is clearly not equal to 5. That is true for all prime numbers.

- Are there any more perfect numbers? The second perfect number is 28. The proper divisors of 28 are 1, 2, 4, 7, and 14, and the sum of those numbers is 28. There are more perfect numbers than just 6 and 28.

- It is unknown whether there are any odd perfect numbers. Up to now, all the perfect numbers that have been discovered are even. In fact, nobody knows if there are an infinite number of perfect numbers. There is a finite number that is known, but perhaps there are more.

PROBLEMS

1. Write the even numbers 22, 24, and 26 as the sum of 2 odd primes.

2. Find a prime gap of length 13.

Fun with Triangular and Square Numbers
Lecture 22

In this lecture, you are going to continue your study of number theory by analyzing 2 types of numbers—square numbers (which are the squares of integers) and triangular numbers (which come from the formula for the sum of the first *n* positive integers)—and some of the relationships between them. You will prove some theorems about them using many of the proof techniques that you have developed thus far, including direct proofs, visual proofs, and proofs by mathematical induction. In addition, you will be introduced to a recursive theorem and its proof.

Triangular versus Square Numbers

- Square numbers are very familiar and easy to understand. They include 1, 4, 9, 16, … . In fact, you can describe square numbers with the following figure.

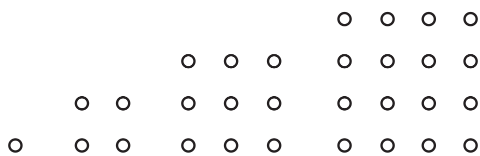


Figure 22.1

- The triangular numbers include 1, 3, 6, 10, … . There are many ways to describe triangular numbers, but one way is with dots that form a triangle, as in the following figure.

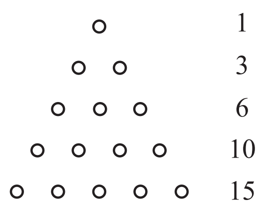


Figure 22.2

- In fact, determining the triangular numbers involves simply adding the first n natural numbers together. This is the summation formula, $\frac{n(n+1)}{2}$, which generates the series 1, 3, 6, 10, 15, 21, … . Note the differences between successive triangular numbers: Triangular numbers differ by 1 more than the previous difference.

- The formal definition for the n^{th} triangular number is $t_n = n(n + 1)/2$. For example, $t_9 = \frac{n(n+1)}{2} = \frac{9(9+1)}{2} = 45.$

The Handshake Problem

- Suppose that you arrive at a party with n people. Everybody must shake hands with everybody else at the party. Given n people, how many handshakes are there?

- For example, if the party has 3 people, then there are 3 handshakes, and with 4 people, there are 6 handshakes. Note that 3 and 6 are triangular numbers. Imagine a party of 10 people. The number of handshakes is 9 + 8 + 7 + … + 2 + 1. That's the ninth triangular number.

- Generalize to n people. If 10 people require the ninth triangular number, then n people require the $n - 1$ triangular number. The n^{th} triangular number is $\frac{n(n+1)}{2}$, so the previous triangular number, t_{n-1}, is the following.

$$t_{n-1} = \frac{(n-1)(n-1+1)}{2} = \frac{(n-1)n}{2}.$$

Relationships between Triangular and Square Numbers

- Add up consecutive triangular numbers. For example, $t_1 + t_2 = 1 + 3 = 4$, $t_2 + t_3 = 3 + 6 = 9$, and $t_3 + t_4 = 6 + 10 = 16$. Notice that the answers are squares. The theorem that was just generated using examples is as follows: $t_{n-1} + t_n = n^2$. For example, $t_2 + t_3 = 3^2 = 9$.

- To prove this theorem, you could use mathematical induction or many other techniques, but it is easiest to do a direct proof. Start with the left-hand side of the equation, do some algebra, and end up with the right-hand side, n^2.

$$\begin{aligned} t_{n-1} + t_n &= \frac{(n-1)n}{2} + \frac{n(n+1)}{2} \\ &= \frac{n^2 - n + n^2 + n}{2} \\ &= \frac{2n^2}{2} = n^2. \end{aligned}$$

- The following visual proof provides another argument. Starting at the top left of the figure, count 1 dot + 2 dots + 3 dots + … + n dots, which is t_n. Counting the remaining dots on the right, from the bottom going upward, yields 1 + 2 + 3 + … + (n − 1), which is t_{n-1}. The total number of dots is $n^2 = t_n + t_{n-1}$.

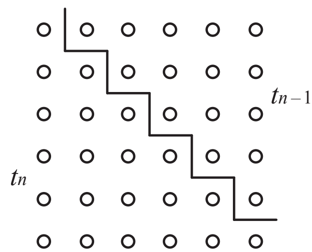


Figure 22.3

- Are there any triangular numbers that are also square numbers? One way to explore this is to make a list of triangular numbers and see if you can spot any square numbers. The first few triangular numbers are 1, 3, 6, 10, 15, 21, 28, 36, 45, … . There are 2 square numbers in the list: 1 and 36. Are there any more?

- The following is a recursive theorem that addresses the overlap of triangular and square numbers: If t_n is square, then so is t_{8t_n}. Note the triple subscript.

- Because t_1 is a square, the theorem tells you that t_8 is also a square. To check this, $t_{8t_1} = t_8 = \frac{8(8+1)}{2} = \frac{72}{2} = 36.$ That's the square that you already knew about.

- Furthermore, given that t_8 is a square, another triangular number that is a square is t_{288}.

$$t_8 = 36 \text{ (square)} \Rightarrow t_{8t_8} = t_{8(36)} = t_{288}$$

$$t_{288} = \frac{288(288+1)}{2} = \frac{83,232}{2} = 41,616 = 204^2 \text{ (square).}$$

- There are an infinite number of triangular numbers that are also perfect squares because the list goes on forever. A direct proof of this theorem is as follows.

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

- Remember that, as part of the hypothesis, t_n itself is a square, so $4t_n$ is a perfect square and so is $(2n + 1)^2$. The whole final answer is indeed a perfect square.

- You now know that you can compute all of these special triangular numbers that are squares, but are there other triangular numbers hiding in the list of all triangular numbers that are squares but aren't given by this theorem? Indeed, there are some that are not on the list. For example, $t_{49} = 1225 = 35^2$.

Sums of Cubes

- Add the cubes as follows and try to find a theorem that relates the outputs.

$$1^3 = 1.$$

$$1^3 + 2^3 = 1 + 8 = 9.$$

$$1^3 + 2^3 + 3^3 = 1 + 8 + 27 = 36.$$

$$1^3 + 2^3 + 3^3 + 4^3 = 1 + 8 + 27 + 64 = 100.$$

- The theorem is that the sums of the cubes are all squares. Furthermore, these squares are squares of triangular numbers. Therefore, the sum of the cubes generates a string of squares of triangular numbers: $1^3 + 2^3 + \ldots + n^3 = (t_n)^2$.

- Use mathematical induction to prove the theorem. To start, the base case, $n = 1$, has already been verified: $1^3 = (t_1)^2$, which is 1^2. Next, assume the theorem is true for n and attempt to prove it for $n + 1$.

$$\begin{aligned}
1^3 + 2^3 + \cdots + n^3 + (n+1)^3 &= (t_n)^2 + (n+1)^3 \\
&= \left[\frac{n(n+1)}{2}\right]^2 + (n+1)^3 \\
&= \frac{n^2(n+1)^2}{4} + (n+1)^3 \\
&= (n+1)^2\left(\frac{n^2}{4} + n + 1\right) \\
&= (n+1)^2\,\frac{(n+2)^2}{4} \\
&= \left[\frac{(n+1)(n+2)}{2}\right]^2 = (t_{n+1})^2.
\end{aligned}$$

More on Triangular Numbers

- There exist right triangles whose sides are triangular numbers. In other words, they satisfy the Pythagorean theorem: t_{132} (8778) and t_{143} (10,296) are the legs of the triangle and t_{164} (13,530) is the hypotenuse. With a calculator, you can verify that those 3 numbers satisfy the Pythagorean theorem. It is still unknown whether there are an infinite number of such Pythagorean triples.

- It was proven in 1989 that there are exactly 5 Fibonacci numbers that are also triangular numbers. It turns out that 1 (t_1), 1 (t_1), 3 (t_2), 21 (t_6), and 55 (t_{10}) are Fibonacci numbers that are also triangular numbers.

PROBLEMS

1. Prove that $9t_n + 1 = t_{3n+1}$.

2. Prove that $t_{n+m} = t_n + t_m + nm$.

Perfect Numbers and Mersenne Primes

Lecture 23

This lecture focuses on the very specific mathematical topic of perfect numbers. In this lecture, you will be exposed to various theorems—including one that was developed by Euclid—and to some unsolved problems. You will also discover the very intimate relationship that exists between perfect numbers and Mersenne primes. As usual, one of the main goals of this lecture is to encourage further study in number theory; in particular, there is a lot of information in the literature about how perfect numbers and Mersenne primes are tied together.

The Study of Perfect Numbers

- If you find the proper divisors of the positive integers and add them, and if they add up to the number itself, then that number is a perfect number.

- The proper divisors (which don't include the number itself) of the positive integer 4 are 1 and 2, for example. The only proper divisor of 5 is 1. In fact, prime numbers only have 1 proper divisor, so none of them are perfect numbers. Because 6 has 3 proper divisors—1, 2, and 3—and the sum of those proper divisors is 1 + 2 + 3 = 6, 6 is a perfect number. It is the first perfect number.

- A natural number n is perfect if it equals the sum of all of its divisors—excluding itself. That is, n is the sum of its proper divisors.

- To aid in the study of perfect numbers, mathematicians have defined a new function called $\sigma(n)$, which is the sum of all of the divisors of a number n. The definition of a perfect number is $\sigma(n) = 2n$.

$$\sigma(3) = 1 + 3 = 4.$$

$$\sigma(4) = 1 + 2 + 4 = 7.$$

$$\sigma(5) = 1 + 5 = 6.$$

$$\sigma(6) = 1 + 2 + 3 + 6 = 12.$$

$$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$$

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56.$$

- After 6, the next perfect number is 28 because $\sigma(28)$ yields the following: $1 + 2 + 4 + 7 + 14 + 28 = 56$, which is 2×28.

- If n is a prime number, then $\sigma(n) = n + 1$. If n is a perfect number, then $\sigma(n) = 2n$. Because you're adding all of the divisors—not just the proper divisors—you include the number n itself, so the sum becomes $n + n$, or $2n$.

- How many perfect numbers exist? A list of the first 6 are as follows.

$$p_1 = 6.$$

$$p_2 = 28.$$

$$p_3 = 496.$$

$$p_4 = 8128.$$

$$p_5 = 33{,}550{,}336.$$

$$p_6 = 8{,}589{,}869{,}056.$$

- Perfect numbers have a rich history. It was very popular among the early Greeks—and, later, in the Middle Ages—to play with perfect numbers. The first 4 perfect numbers were known to the early Greeks. In 1456, in the Middle Ages, p_5 was discovered. In 1588, p_6 and p_7 were discovered.

- As of 2011, there are 47 perfect numbers known. The largest known perfect number has 25,956,377 digits—almost 26 million digits.

- The last digit of the first 5 perfect numbers shows a pattern of 6, 8, 6, 8, 6, but p_6 breaks that pattern with a 6 as its final digit. Interestingly, however, it can be shown that the last digit of every even perfect number ends in either a 6 or an 8.

- All of the 47 known perfect numbers are, in fact, even. However, nobody knows whether an odd perfect number exists. It's another unsolved problem. In addition, nobody seems to know whether there is an infinite number of perfect numbers.

Perfect Numbers and Mersenne Primes

- Euclid studied perfect numbers. In fact, some of his books are devoted to number theory. The following theorem deals with perfect numbers: If $p = 2^k - 1$ is a prime number, then $2^{k-1}p$ is a perfect number.

- Do you believe this theorem? Try some examples.

$$p = 2^2 - 1 = 3 \text{ (prime)} \Rightarrow 2^{2-1}(3) = 6 \text{ (perfect)}.$$
$$p = 2^3 - 1 = 7 \text{ (prime)} \Rightarrow 2^{3-1}(7) = 28 \text{ (perfect)}.$$
$$p = 2^5 - 1 = 31 \text{ (prime)} \Rightarrow 2^{5-1}(31) = 496 \text{ (perfect)}.$$

- The hypothesis of Euclid's theorem is that a number of the form $2^k - 1$ has to be a prime number. Prime numbers of the form $2^k - 1$ are known as Mersenne primes, which are named after a 17th-century French monk who studied these kinds of prime numbers.

- Are there other Mersenne primes? As of 2011, there are 47 known Mersenne primes. There are also 47 known perfect numbers. Mersenne primes and perfect numbers seem to be intimately tied together.

- Some examples of Mersenne primes are $2^2 - 1 = 3$, $2^3 - 1 = 7$, and $2^5 - 1 = 31$. If you keep computing these, you will find that 127, 8191, and 131,071 are Mersenne primes.

- It can be shown that if $2^k - 1$ is a prime, then so is k. Early mathematicians thought that $2^k - 1$ would be prime for all prime numbers k, but that is not true.

- In 1536, Hudalrichus Regius discovered that $2^{11} - 1$ (11 is a prime number) is not a Mersenne prime because you can factor it: $2^{11} - 1 = 2047 = 23 \times 89$. Therefore, the idea that for every prime k, $2^k - 1$ is a prime is false. Amazingly, Regius did this computation using Roman numerals and an abacus.

- Remember that Euclid's proof states that if $p = 2^k - 1$ is a prime number—or a Mersenne prime—then $2^{k-1}p$ is a perfect number. To prove this, you will need a few little theorems, called lemmas, that are useful in subdividing the main proof.

- The first lemma is the following: If a and b are 2 positive integers with no common factors (if they are relatively prime), then $\sigma(ab) = \sigma(a)\sigma(b)$. Recall that σ is the sum of all of the divisors.

- To illustrate this theorem, do a few examples. Then, you become confident that it is, in fact, a theorem. (The proof is not difficult, but it is omitted because it is uninteresting.) For example, suppose that $a = 3$ and $b = 4$.

$$\sigma(3) = 1 + 3 = 4.$$
$$\sigma(4) = 1 + 2 + 4 = 7.$$
$$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$$
$$\sigma(12) = \sigma(3)\sigma(4).$$

- Next, suppose that $a = 4$ and $b = 7$.

$$\sigma(4) = 1 + 2 + 4 = 7.$$
$$\sigma(7) = 1 + 7 = 8.$$
$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56.$$
$$\sigma(28) = \sigma(4)\sigma(7).$$

- The second lemma that you need before attempting the main proof states that if p is a prime number, then the following is true.

$$\sigma(p) = 1 + p.$$
$$\sigma(p^2) = 1 + p + p^2.$$
$$\sigma(p^3) = 1 + p + p^2 + p^3.$$
$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

- The following example will be needed in the proof of Euclid's theorem. Instead of the power k, use the power $k - 1$; it's still the same theorem—except for that replacement.

$$\sigma(2^{k-1}) = \frac{2^{(k-1)+1} - 1}{2 - 1} = \frac{2^k - 1}{1} = 2^k - 1.$$

- In order to do the direct proof of Euclid's theorem, assume that $p = 2^k - 1$ is prime. You want to show that $2^{k-1}p = n$ is perfect. That is, you want to show that $\sigma(n) = 2n$.

$$\begin{aligned} n &= 2^{k-1} p = 2^{k-1}(2^k - 1) \\ \sigma(n) &= \sigma(2^{k-1})\sigma(2^k - 1) \ (\text{because they are relatively prime}) \\ &= \frac{2^k - 1}{2 - 1}(2^k - 1 + 1) \ (\text{because } 2^k - 1 \text{ is prime}) \\ &= (2^k - 1)(2^k) \\ &= 2(2^{k-1})(2^k - 1) = 2n. \end{aligned}$$

- Euclid extended this theorem; he made it an if-and-only-if theorem: $p = 2^k - 1$ is prime if and only if $2^{k-1}p$ is perfect. He was able to prove that there is a one-to-one correspondence between Mersenne primes and the even perfect numbers.

- Today, there are 47 known perfect numbers and 47 known Mersenne primes, and there is a one-to-one correspondence between them. Therefore, if you find a new Mersenne prime, you will find a new perfect number, and vice versa.

PROBLEMS

1. Calculate $\sigma(125)$, $1 + 5 + 5^2 + 5^3$, and $\frac{5^4 - 1}{5 - 1}$. What do you observe?

2. Verify that $\sigma(14) = \sigma(2)\sigma(7)$.

Let's Wrap It Up—The Number e

Lecture 24

This final lecture will focus on the famous number *e*, which plays a role in mathematics that is similar to the role that is played by the number π—but it's perhaps even more important. It is a real number with an unending string of decimals. The number *e* is a number that has enormous applications, and it plays a crucial role in precalculus and calculus courses. In this lecture, you will prove some properties about *e*, including the fact that it is an irrational number.

Defining *e*

- Suppose that you invest \$1 in an amazing bank that pays 100% interest annually. How much money would you have after 1 year? Of course, \$2. Your money would double because the interest rate is 100%.

- If the interest is compounded every 6 months (semiannually), you would use the following formula for compound interest to determine how much money you would have after 1 year.

- $A = P\left(1+\frac{r}{n}\right)^{nt} = \left(1+\frac{1}{n}\right)^{n}$, where A is the amount of money in the account, P is the principal, r is the interest rate (in decimal form), *n* is the number of compoundings per year, and *t* is the time in years.

- Applying the formula with $n = 2$ (because the money is compounded twice per year), you would have \$2.25 in your bank account after 1 year.

$$A = P\left(1+\frac{r}{n}\right)^{nt} = \left(1+\frac{1}{n}\right)^{n} = \left(1+\frac{1}{2}\right)^{2} = 2.25.$$

- The following is the result of the bank compounding interest monthly, daily, and hourly—respectively.

$$A = P\left(1+\frac{r}{n}\right)^{nt} = \left(1+\frac{1}{n}\right)^{n} = \left(1+\frac{1}{12}\right)^{12} \approx 2.61.$$

$$A = \left(1+\frac{1}{365}\right)^{365} \approx 2.71.$$

$$A = \left(1+\frac{1}{8760}\right)^{8760} \approx 2.71813.$$

- These 3 numbers seem to be approaching the constant 2.718 … . In fact, Jacob Bernoulli, one of the many Bernoulli mathematicians, observed that this approaches a limit as the number of compoundings increases. That limit is the number *e*.

- One possible definition of the number *e* involves analyzing the expression $(1 + 1/n)^n$ for various values of n as n approaches infinity.

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

$$\left(1+\frac{1}{2}\right)^{2} = 2.25.$$

$$\left(1+\frac{1}{100}\right)^{100} \approx 2.7048.$$

$$\left(1+\frac{1}{10,000}\right)^{10,000} \approx 2.718146.$$

- Mathematicians say that e is the limit as n approaches infinity: $e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^{n}$.

- Another way of defining the number e involves using factorials. Recall the following.

$$n! = n(n-1)(n-2)\ldots(3)(2)(1)$$

$$1! = 1$$

$$2! = 2(1) = 2$$

$$3! = 3(2)(1) = 6$$
$$4! = 4(3)(2)(1) = 24$$
$$5! = 120$$
$$0! = 1$$

- In general, $\frac{n!}{(n-1)!} = n.$

$$1 + \frac{1}{1!} = 2.$$

$$1 + \frac{1}{1!} + \frac{1}{2!} = 2.5.$$

$$1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} \approx 2.667.$$

$$\frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \ldots + \frac{1}{10!} \approx 2.71828\ldots.$$

- What do you observe? These values are approaching a fixed number, and that number is e.

$$\begin{aligned} e &= \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \ldots \\ &= \sum_{n=0}^{\infty} \frac{1}{n!}. \end{aligned}$$

- The number e is crucial for all of mathematics. Like π, e is a never-ending, nonrepeating decimal. In fact, e is an irrational number. It is built into calculators. The exponential function is e^x, and its inverse is the natural logarithm function $\ln(x)$. It could be argued that e is the most important number in mathematics.

- The number e has many applications, including applications to compound interest and growth and decay problems (such as radioactive decay).

- The formula for the amount of money you would have in a bank that compounds continuously is $A = Pe^{rt}$.

- In calculus, e is the amazing function whose derivative is equal to itself: $\frac{d}{dx}\left[e^x\right] = e^x$.

- In addition, $e^{i\pi} = -1$, where i is $\sqrt{-1}$. This formula links e, i, and π—perhaps the 3 most important numbers. Written differently, $1 + e^{i\pi} = 0$ or $-e^{i\pi} = 1$.

- These properties about e are often proved in upper-level math courses such as differential equations.

The Nature of the Number *e*

- Prove that e is an irrational number. Assume by way of contradiction that e is rational—that it's a fraction. Then, use the series definition of e (the one involving factorials) to derive a contradiction.

- If e is rational, then it's of the form p/q, where p and q are positive integers, and e is positive, so you can assume that $q > 1$: $e = p/q$, $q > 1$. If q was 1, then e would be an integer, and that is not true.

- Next, derive a contradiction. Based on the series definition of e, the following is true.

$$\begin{aligned}\frac{p}{q} = e &= \frac{1}{0!}+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\ldots \\ &= \frac{1}{0!}+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\ldots+\frac{1}{q!}+\frac{1}{(q+1)!}+\frac{1}{(q+2)!}+\ldots \\ &= \sum_{n=0}^{q}\frac{1}{n!}+\sum_{n=q+1}^{\infty}\frac{1}{n!}.\end{aligned}$$

$$\frac{p}{q}-\sum_{n=0}^{q}\frac{1}{n!} = \sum_{n=q+1}^{\infty}\frac{1}{n!}$$

- Then, multiply both sides of the equation by $q!$.

$$q!\left(\frac{p}{q}-\sum_{n=0}^{q}\frac{1}{n!}\right)=q!\left(\sum_{n=q+1}^{\infty}\frac{1}{n!}\right)$$

$$\left(\frac{pq!}{q}-\sum_{n=0}^{q}\frac{q!}{n!}\right)=\left(\sum_{n=q+1}^{\infty}\frac{q!}{n!}\right)=\frac{q!}{(q+1)!}+\frac{q!}{(q+2)!}+\ldots.$$

- The left-hand side of the equation, $\left(\frac{pq!}{q}-\sum_{n=0}^{q}\frac{q!}{n!}\right)$, is a positive integer. The contradiction is that the right-hand side, $\frac{q!}{(q+1)!}+\frac{q!}{(q+2)!}+\ldots$, is not a positive integer, which is proven as follows.

$$\frac{q!}{(q+1)!}+\frac{q!}{(q+2)!}+\ldots$$

$$=\frac{1}{q+1}+\frac{1}{(q+1)(q+2)}+\frac{1}{(q+1)(q+2)(q+3)}+\ldots$$

$$<\frac{1}{q+1}+\frac{1}{(q+1)^2}+\frac{1}{(q+1)^3}+\ldots.$$

- That final expression is a geometric series. Recall the formula for an infinite geometric series: $1 + r + r^2 + r^3 + \ldots = \frac{1}{1-r}$, as long as r is between -1 and 1. That infinite geometric series is derived from the finite geometric series, which is $1 + r + r^2 + \ldots + r^n = \frac{1-r^{n+1}}{1-r}$.

- If you factor out $\frac{1}{q+1}$, what remains looks just like the formula, where $r=\frac{1}{q+1}$, so the theorem applies.

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

- Then, use the formula for a geometric series.

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

Hence,

$$\left(\frac{pq!}{q}-\sum_{n=0}^{q}\frac{q!}{n!}\right)=\frac{q!}{(q+1)!}+\frac{q!}{(q+2)!}+\ldots<\frac{1}{q}.$$

- In conclusion, the left-hand side is a positive integer, and the right-hand side is less than $1/q$ (or between 0 and 1), which is the contradiction. Hence, e is irrational.

- It turns out that e is not only irrational, but it is also transcendental, which is a number that is not the root of any polynomial equation with rational coefficients. It also turns out that π is transcendental, but it is not known whether $e+\pi$ is transcendental.

PROBLEMS

1. Which is larger, π^e or e^π?

2. The infinite series for $f(x) = e^x$ is $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots$. Differentiate this series term by term. What do you observe?

Solutions

LECTURE 1

1. Let $2n$ be an even number and $2m + 1$ be an odd number. Their sum is $2n + 2m + 1 = 2(n + m) + 1$, which is an odd number.

2. A mathematical proof is based on logic and deductive reasoning. A proof establishes the validity of a statement for all possible cases. In other disciplines, proofs might be based on statistical evidence or theories. Answers will vary.

LECTURE 2

1. The angle bisector $\overline{AD}$ divides the original triangle into 2 triangles. These triangles are congruent by side-angle-side: $\Delta BAD \cong \Delta CAD$. Hence, the angles at B and C are congruent: $\angle ABC \cong \angle ACB$.

2. Let ΔABC be given, with $\angle A$ congruent to $\angle B$. Then, by angle-side-angle, ΔCAB is congruent to ΔCBA. Thus, $CA = CB$, and the triangle is isosceles.

LECTURE 3

1. This statement means 2 things: a is greater than or equal to b, and b is greater than c.

2. The tables are the same. The expressions are equivalent.

P	*Q*	*R*	*P* and *Q*	(*P* and *Q*) or *R*
T	T	T	T	**T**
T	T	F	T	**T**
T	F	T	F	**T**
T	F	F	F	**F**
F	T	T	F	**T**
F	T	F	F	**F**
F	F	T	F	**T**
F	F	F	F	**F**

P	*Q*	*R*	*P* or *R*	*Q* or *R*	(*P or R*) and (*Q or R*)
T	T	T	T	T	**T**
T	T	F	T	T	**T**
T	F	T	T	T	**T**
T	F	F	T	F	**F**
F	T	T	T	T	**T**
F	T	F	F	T	**F**
F	F	T	T	T	**T**
F	F	F	F	F	**F**

LECTURE 4

1. The tables are not the same. The expressions are not equivalent.

P	*Q*	*P* implies *Q*
T	T	**T**
T	F	**F**
F	T	**T**
F	F	**T**

P	*Q*	Not *P*	Not *Q*	(Not *P*) implies (Not *Q*)
T	T	F	F	**T**
T	F	F	T	**T**
F	T	T	F	**F**
F	F	T	T	**T**

2. The tables are the same. The expressions are equivalent.

P	*Q*	*P* or *Q*	Not (*P* or *Q*)
T	T	T	**F**
T	F	T	**F**
F	T	T	**F**
F	F	F	**T**

P	*Q*	Not *P*	Not *Q*	(Not *P*) and (Not *Q*)
T	T	F	F	**F**
T	F	F	T	**F**
F	T	T	F	**F**
F	F	T	T	**T**

LECTURE 5

1. This is false. There is no largest real number.

2. $\left\{\frac{n+1}{n}\right\}: 2, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \frac{6}{5}.$ The limit is 1.

$\left\{(-1)^n\right\}: -1, 1, -1, 1, -1.$ The limit does not exist.

LECTURE 6

1. Let $x = 2n+1$ and $y = 2m+1$ be 2 odd integers. Then, their product is $xy = (2n + 1)(2m + 1) = 4nm + 2n + 2m + 1 = 2(2nm + n + m) + 1$, which is odd.

2. Recall that an inequality is reversed if both sides are multiplied by a negative number. First, multiply $a < b$ by a and then $a < b$ by b as follows: $a < b \Rightarrow a^2 > ab$ and $a < b \Rightarrow ab > b^2$. Hence, $a^2 > ab > b^2 \Rightarrow a^2 > b^2$.

3. First, factor out the nonzero constant a and then complete the square, as follows.

$$
\begin{aligned}
ax^2 + bx + c &= 0 \\
a\left(x^2 + \frac{b}{a}x\right) &= -c \\
a\left(x^2 + \frac{b}{a}x + \frac{b^2}{4a^2}\right) &= -c + \frac{b^2}{4a} \\
a\left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a} \\
\left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \\
x + \frac{b}{2a} &= \frac{\pm\sqrt{b^2 - 4ac}}{2a} \\
x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}
\end{aligned}
$$

LECTURE 7

1. Suppose, by way of contradiction, that n is even. Then, $n = 2m$ and $n^2 = 4m^2 = 2(2m^2)$ is even. This is a contradiction, so n must be odd.

2. First show that if n^2 is a multiple of 3, then so is n. Suppose, by way of contradiction, that n is not a multiple of 3. Then, $n = 3m + 1$ and $n^2 = 9m^2 + 6m + 1$, or $n = 3m + 2$ and $n^2 = 9m^2 + 12m + 4$. In both cases, n^2 is not a multiple of 3, so you have a contradiction. To prove that the square root of 3 is irrational, suppose, by way of contradiction, that it is rational. Then, $\sqrt{3} = a/b$ where the integers a and b have no common factors. Squaring both sides, you obtain $3 = \frac{a^2}{b^2} \Rightarrow a^2 = 3b^2$.

Hence, a^2 is a multiple of 3, and thus, a is also a multiple of 3: $a = 3c$. Then, you have $a^2 = (3c)^2 = 9c^2 = 3b^2 \Rightarrow 3c^2 = b^2$. By the same argument, b is a multiple of 3. Thus, a and b have a common factor, which is a contradiction.

LECTURE 8

1. This is an if-and-only-if proof. On one hand, if both m and n are odd, then you have $mn = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1$, which is odd. On the other hand, assume that mn is odd. Use a proof by contradiction to show that both m and n are odd. If either one were even, then the product would be even, which is a contradiction.

2. On one hand, if n is divisible by 3, then $n = 3m$ and $n^2 = 9m^2 = 3(3m^2)$ is divisible by 3. On the other hand, if n^2 is divisible by 3, then it is a multiple of 3. The proof of Problem 2 from Lecture 7 shows that n is a multiple of 3.

LECTURE 9

1. Show that each set is a subset of the other. Let $x \in (A \cup B)'$. Then, $x \notin (A \cup B)$. Therefore, $x \notin A$ and $x \notin B$. Thus, $x \in A'$ and $x \in B'$ $\Rightarrow x \in A' \cap B'$. Next, let $x = A' \cap B'$. Then, $x \in A'$ and $x \in B'$. Thus, $x \notin A$ and $x \notin B$, which implies that $x \notin (A \cup B) \Rightarrow x \in (A \cup B)'$.

2. $A \cup B = \{a, b, x, y\}$; $A \cap B = \{a, x\}$; $A' = \{c, y, x\}$; $A \cup A' = U$; $A \cap A' = \phi$.

LECTURE 10

1. A bijection between the positive integers and the even positive integers is given by $f(n) = 2n$.

2. If the irrational numbers were countable, then the union of the rational numbers and irrational numbers would be countable. However, the real numbers are not countable.

LECTURE 11

1. The base case $1^2 = \frac{1(1+1)(2+1)}{6}$ is verified. Next, assume that the formula is true for n. Show that the formula is true for n + 1. In this case, the right-hand side of the equation is $\frac{(n+1)(n+2)(2(n+1)+1)}{6}$ = $\frac{(n+1)(n+2)(2n+3)}{6}$. Begin with the left-hand side.

$$
\begin{aligned}
1^2 + 2^2 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= \frac{n+1}{6}\left[n(2n+1) + 6(n+1)\right] \\
&= \frac{n+1}{6}\left[2n^2 + 7n + 6\right] \\
&= \frac{n+1}{6}\left[(n+2)(2n+3)\right] = \frac{(n+1)(n+2)(2n+3)}{6}.
\end{aligned}
$$

2. The base case $1 \le 2^1$ is verified. Next, assume that the statement is true for n. Then, you have $n+1 \le 2^n + 1 < 2^n + 2 = 2^{n+1} \Rightarrow n+1 \le 2^{n+1}$, which shows that the statement is true for n + 1.

LECTURE 12

1. The base case $2|(1^2 + 1)$ is verified. Next, assume that the property is true for n. That is, assume that $2|(n^2 + n)$. You have to show that 2 divides $\left[(n+1)^2 + (n+1)\right]$. This expression simplifies to $n^2 + 2n + 1 + n + 1 = (n^2 + n) + (2n + 2)$.

By the induction hypothesis, 2 divides the first term, and 2 clearly divides the second term. Hence, 2 divides their sum, as desired.

2. The hypothesis implies that there exist integers m and n such that $b = an$ and $c = am$. Thus, $b + c = an + am = a(m + n)$ shows that $a|(b + c)$.

LECTURE 13

1. $95 = 5 \times 19$

$$96 = 2 \times 48 = 2 \times 2 \times 24 = 2 \times 2 \times 2 \times 12 =$$
$$= 2 \times 2 \times 2 \times 2 \times 6 = 2 \times 2 \times 2 \times 2 \times 2 \times 3 = 2^5 \times 3.$$

2. $$\alpha^2 = \left(\frac{1-\sqrt{5}}{2}\right)^2 = \left(\frac{1-2\sqrt{5}+5}{4}\right) = \frac{3-\sqrt{5}}{2} = \frac{1-\sqrt{5}}{2} + 1 = \alpha + 1.$$

LECTURE 14

1. Suppose, by way of contradiction, that $z = a + bx$ is rational. Then, solving for x, you obtain $x = \frac{z-a}{b}$, which is a rational number. This contradicts the hypothesis.

2. You can use the intermediate value theorem to determine that the function has 3 zeros. They are located on the intervals $[-1,0]$, $[0,1]$, and $[2,3]$.

3. Consider $x=\left(\sqrt{2}\right)^{\sqrt{2}}$. If this number is irrational, then you are done. If not, then consider the number $x\sqrt{2}=\left(\sqrt{2}\right)^{\sqrt{2}+1}$. Next, use Problem 1 twice: Because x is rational and $\sqrt{2}$ is irrational, their product is irrational. Also, $\sqrt{2}+1$ is irrational. Letting $a=\sqrt{2}$ and $b=\sqrt{2}+1$, a^b is equal to an irrational number, $x\sqrt{2}$.

LECTURE 15

1. By long division, you obtain 503 = 9(55) + 8.

2. By factoring, you find that $(x+1)^2=0 \Rightarrow x+1=0 \Rightarrow x=-1$ is the unique solution.

LECTURE 16

1. There are 4 cases to consider: both numbers are positive, both numbers are negative, and the 2 cases in which the numbers differ in sign. Consider each case in turn.

If both numbers are positive, then $\left|\frac{x}{y}\right|=\frac{x}{y}=\frac{|x|}{|y|}$.

If both numbers are negative, then $\frac{x}{y}$ is positive and $\left|\frac{x}{y}\right|=\frac{x}{y}=\frac{-x}{-y}=\frac{|x|}{|y|}$.

If the numerator is negative and the denominator is positive, then $\left|\frac{x}{y}\right|=-\left(\frac{x}{y}\right)=\frac{-x}{y}=\frac{|x|}{|y|}$.

If the numerator is positive and the denominator is negative, then $\left|\frac{x}{y}\right|=-\left(\frac{x}{y}\right)=\frac{x}{-y}=\frac{|x|}{|y|}$.

2. There are 3 cases; consider each case in turn.

If $m = 3a + 1$ and $n = 3b + 1$, then $mn = (3a + 1)(3b + 1) = 9ab + 3a + 3b + 1$, which is not divisible by 3.

If $m = 3a + 1$ and $n = 3b + 2$, then $mn = (3a + 1)(3b + 2) = 9ab + 6a + 3b + 2$, which is not divisible by 3.

If $m = 3a + 2$ and $n = 3b + 2$, then $(3a + 2)(3b + 2) = 9ab + 6a + 6b + 4$, which is not divisible by 3.

LECTURE 17

1. This is false. Let $n = 11$. Then, $2^{11} - 1 = 2047 = 23 \times 89$.

2. This is false because $x^4 + 2x^2 + 1 = \left(x^2 + 1\right)^2 > 0$ for all x.

LECTURE 18

1. There is a division by 0 between lines 2 and 3.

2. This is a false proof because the first line is actually the conclusion of the proof.

LECTURE 19

1. There are many possible answers. One counterexample is $A = \{a, b\}, B = \{c\}$ and $C = \{b, d\}$. Then, $A \cap \left(B \cup C\right) = \{b\}$ whereas $\left(A \cap B\right) \cup C = \{b, d\}$.

2. The sum of the first 100 odd natural numbers is $100^2 = 10{,}000$. The sum of the first 200 natural numbers is $\frac{200(201)}{2} = 20{,}100$. Hence, the sum of the first 100 even natural numbers is $20{,}100 - 10{,}000 = 10{,}100$.

LECTURE 20

1. The factorization of 30,030 = 2 × 3 × 5 × 7 × 11 × 13. The factorization of 1537 = 29 × 53, which is more difficult.

2. There are 21 prime numbers between 100 and 200: 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, and 199.

LECTURE 21

1. There are many ways to do this. For example, 22 = 11 + 11 = 19 + 3 = 17 + 5, 24 = 11 + 13 = 7 + 17 = 5 + 19, and 26 = 13 + 13 = 7 + 19 = 3 + 23.

2. You could use the theorem on prime gaps. From the list of primes between 100 and 200, there is a gap of length 13 between the primes 113 and 127.

LECTURE 22

1. You can use a direct proof, as follows.

$$\begin{aligned} 9t_n + 1 &= 9\left(\frac{n(n+1)}{2}\right) + 1 = \frac{9n(n+1)+2}{2} \\ &= \frac{9n^2 + 9n + 2}{2} = \frac{(3n+1)(3n+2)}{2} = t_{3n+1}. \end{aligned}$$

2. You can use a direct proof, as follows.

$$\begin{aligned} t_{n+m} &= \frac{(n+m)(n+m+1)}{2} = \frac{n^2 + nm + n + mn + m^2 + m}{2} \\ &= \frac{n^2+n}{2} + \frac{m^2+m}{2} + nm = t_n + t_m + nm. \end{aligned}$$

LECTURE 23

1. All 3 equal 156, which is guaranteed by the formula in this lecture.

2. You find that the 2 sides are equal.

$$\sigma(14) = 1 + 2 + 7 + 14 = 24.$$
$$\sigma(2)\sigma(7) = (1+2)(1+7) = 3(8) = 24.$$

LECTURE 24

1. Using a calculator, you can verify that $e^{\pi} \approx 23.14 > \pi^{e} \approx 22.46$.

2. If you differentiate term by term, the resulting series is exactly the same as what is given. This confirms the property that the derivative of the exponential function equals itself.

Bibliography

Alsina, Claudi, and Roger B. Nelsen. *Charming Proofs: A Journey into Elegant Mathematics*. Dolciani Mathematical Expositions #42. Washington, DC: The Mathematical Association of America, 2010. This is a more difficult book that has many geometric proofs.

Bloch, Ethan D. *Proofs and Fundamentals*. Boston: Birkhäuser, 2000. This is a fairly high-level textbook focusing on the transition from calculus to higher mathematics courses.

Cupillari, Antonella. *The Nuts and Bolts of Proofs*. 3rd ed. Boston: Elsevier, 2005. This small textbook provides an excellent introduction to proofs.

Daepp, Ulrich, and Pamela Gorkin. *Reading, Writing, and Proving: A Closer Look at Mathematics*. New York: Springer, 2003. For a beginner's book about proof techniques, this textbook covers many fields of mathematics.

Devlin, Keith. *Sets, Functions, and Logic*. 3rd ed. Boca Raton, FL: Chapman & Hall/CRC, 2004. This is a higher-level textbook on proofs that has chapters on functions and relations.

Eccles, Peter J. *An Introduction to Mathematical Reasoning*. Cambridge: Cambridge University Press, 2007. This is a very readable textbook on proofs that has material on Diophantine equations and modular arithmetic.

Garnier, Rowan, and John Taylor. *100% Mathematical Proof*. New York: John Wiley and Sons, 1996. This textbook provides a formal introduction to proof theory via logic.

Hale, Margie. *Essentials of Mathematics*. Washington, DC: The Mathematical Association of America, 2003. This slim volume for first- and second-year college students covers logic and number systems. There is also valuable discussion on the overall field of mathematics.

Hardy, G. H. *A Mathematician's Apology*. Cambridge: Cambridge University Press, 1948. This wonderful little book offers a strong defense of pure mathematics.

Larson, Ron, Robert Hostetler, and Bruce Edwards. *Precalculus, A Graphing Approach*. 5th ed. Boston: Houghton Mifflin, 2008. This textbook provides a thorough coverage of precalculus, including the major theorems and proofs from algebra and trigonometry

Larson, Ron, and Bruce Edwards. *Calculus*. 9th ed. Belmont, CA: Brooks/Cole, 2010. This best-selling textbook contains the major theorem and proofs from elementary calculus.

Lavine, Shaughan. *Understanding the Infinite*. Cambridge, MA: Harvard University Press, 1994. This book provides a very complete and accessible treatment of infinity, Cantor's work, and the axiom of choice.

Polster, Burkard. *Q.E.D.: Beauty in Mathematical Proof*. New York: Walker and Company, 2004. This tiny book offers many interesting visual proofs, especially in geometry.

Polya, George. *How to Solve It*. Princeton, NJ: Princeton University Press, 1945. This is a classic book on problem solving that contains excellent advice on how to discover solutions.

———. *Induction and Analogy in Mathematics.* Vol. I, *Mathematics and Plausible Reasoning*. Princeton, NJ: Princeton University Press, 1954. This is a classic book on mathematical reasoning that covers all areas of mathematics.

———. *Patterns of Plausible Inference.* Vol. II, *Mathematics and Plausible Reasoning*. Princeton, NJ: Princeton University Press, 1954. This is the second volume of Polya's classic series on mathematical reasoning.

Solow, Daniel. *How to Read and Do Proofs*. 5th ed. Hoboken, NJ: John Wiley and Sons, 2010. This compact textbook gives a thorough introduction to the art of proofs, including proofs from discrete mathematics, linear algebra, and real analysis.

Sundstrom, Ted. *Mathematical Reasoning, Writing, and Proof*. 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2007. This very readable textbook provides excellent coverage of proof theory in the area of functions, equivalence relations, and number theory.

Velleman, Daniel J. *How to Prove It*. 2nd ed. Cambridge: Cambridge University Press, 2006. This textbook covers proofs from a more structured, or algorithmic, approach. There is a valuable chapter on functions and their proofs.

Internet Resource

Wolfram MathWorld. http://mathworld.wolfram.com. Wolfram MathWorld is a resource for all areas of mathematics.

Notes

Notes

Notes