2. Proofs

Key Terms and Definitions

- even and odd integers
- parity
- rational numbers

Symbols

Symbol	Description
$x \mid y$	x divides y
$x \nmid y$	x does not divide y
$\in$	Belongs to
■	Indicates end of proof
$\therefore$	Means "therefore"

2.1 Mathematical Definitions

- Definitions related to mathematical objects
- Basic mathematical concepts useful in proofs
- Definition of even and odd integers with algebraic expressions.

Even and odd integers

> An integer x is even if there is an integer k such that x = 2k.
> An integer x is odd if there is an integer k such that x = 2k+1

Parity

- Parity refers to the odd or even nature of a number.
- If two numbers are both odd or both even, they have the same parity.

- If one number is odd and the other is even, then they have opposite parity.

O(x): x is odd P(x, y): x and y have same parity $P(x, y) = O(x) \leftrightarrow O(y)$

Rational numbers

- A rational number can be expressed as the ratio of two integers, where the denominator is not zero.
- The choice of integers used to represent a rational number is not necessarily unique.
- For instance, the rational number 0.5 can be represented as 1/2 or 2/4.

Divides

- An integer x can divide another integer y if x is not zero and y can be written as k times x, where k is also an integer.
- We use the symbol $x|y$ to mean that x <u>divides</u> y.
- If x cannot divide y, we use the symbol $x\nmid y$.
- When y is a <u>multiple</u> of x, it means that x is one of the numbers that can divide y.
- We call x a <u>factor</u> or <u>divisor</u> of y.

Prime and composite numbers

- An integer n is called a <u>prime number</u> if it is greater than 1 and only 1 and n can divide it.

- An integer n is called a <u>composite number</u> if it is greater than 1 and can be divided by at least one positive integer other than 1 and itself.

- There is no known formula that can determine whether a given number x is prime or not.

- However, there are algorithms that can test whether a number is prime, such as the Sieve of Eratosthenes and the Miller-Rabin primality test.

Inequalities

- When we compare two numbers x and c, one of three things is true:
  $x < c$
  $x = c$
  $x > c$

- We use symbols like $<$, $>$, $\leq$, and $\geq$ to show how x and c are related.

- For example, $x \geq c$ means x is at least as big as c, and $x \leq c$ means x is at most as big as c.

- If we say "not $x < c$", that means x is at least as big as c ($x \geq c$) or x is greater than or equal to c.

- if we say "not $x > c$", that means x is at most as big as c ($x \leq c$) or is less than or equal to c.

- A positive number is greater than zero, a negative number is less than zero, a non-negative number is greater than or equal to zero, and a non-positive number is less than or equal to zero.

2.2 Introduction to proofs

Theorems

- In math, we try to prove things called theorems. A theorem is like a big puzzle piece that we have to fit into place.
- To prove a theorem, we use logic and reasoning to show that it's true. We start with things that we know are true, and use them to figure out if the theorem is also true.

- Sometimes we have to use special rules called axioms, which are things we just assume are true, like "if A = B and B = C, then A = C".
- Proofs are important in computer science too! We use them to make sure that computer programs work correctly, or to check that a system for keeping secrets (called a cryptosystem) is safe from hackers.

Example Theorem

Statement
Every positive integer is less than or equal to its square.

Expression
$\forall x \; (\; (\; x > 0 \;) \rightarrow (\; x \leqq x^2 \;) \;)$

Theorems that are universal or existential statements

Universal statements:

- Most theorems are universal statements, which assert something about all elements in a set.

- Universal statements might not use words like "for all" or "for every".

- Example: "The sum of two positive real numbers is strictly greater than the average of the two numbers."

- In logic, this statement can be expressed as:

$$\forall x \forall y(\; (\; x > 0 \land y > 0 \;) \rightarrow (\; x + y \;) > \frac{(\; x + y \;)}{2} \;)$$

Existential statements:

- Some theorems are existential statements, which assert the existence of a number or object with certain properties.

- Example: "There is an integer that is equal to its square."

- In logic, this statement can be expressed as:

$$\exists x(x = x^2)$$

Understanding whether a theorem is a universal or existential statement is an important first step in proving that the theorem is true.

Example: perfect square

- A number n is a perfect square if n = k^2 for some integer k.
- Existentially: "There is a perfect square that is the sum of two non-zero perfect squares".

Let
P(x): x is a perfect square

Expression
$\exists x \exists y \exists z\ ((P(x) = P(y) + P(z)) \wedge (\ y \neq 0 \wedge z \neq 0\ ))$

Proofs of universal statements: proofs by exhaustion

- Small domains may be easier to prove by checking each element individually.
- This kind of proof is called a proof by exhaustion.

Example

If $n \in \{ -1, 0, 1 \}$, then $n^2 = | n |$

Check the equality for each possible value of n:

n = -1: $(-1)^2 = 1 = |-1|$
n = 0: $(0)^2 = 0 = |0|$
n = 1: $(1)^2 = 1 = |1|$

All equalities are true.

Proofs of universal statements: universal generalization

- Universal statement is difficult to prove individually for each element in the domain
- Universal generalization is the most common method for proving universal statements
- A proof using universal generalization names an arbitrary object in the domain and proves the statement for that object
- "Arbitrary" means nothing is assumed about the object other than the assumptions given in the statement.

> **Theorem**
> Every positive integer is less than or equal to its square.
>
> Proof
> Let x be an (arbitrary) integer such that $x > 0$
> So x must be greater than or equal to 1.
> ($x \geqq 1$)
> $\therefore \quad x^2 \geqq x$

Tips for providing a general overview of proof complexity

- Including explicit statements within the proof to indicate the intended direction can be useful.
- For example, a proof of x ≤ x2 could begin with the statement "We shall show that x ≤ x2."
- It is recommended to write down the fact being proved in precise mathematical language within one's preliminary work to ensure that the reasoning process leads to the desired outcome.

Definition of consecutive integers

- Two integers are considered consecutive if one of the integers is equivalent to the other plus one.
- For instance, 4 and 5 are consecutive integers.
- However, 4 and 6, as well as 4 and 4, are not consecutive integers.

Counterexamples

- Proving a universal statement for each element in a large or infinite domain is impractical.
- Giving examples to prove a universal statement is unreliable because there can always be a counterexample that was not tried.
- A counterexample is an assignment of values to variables that shows that a universal statement is false.
- The only way to be certain that a universal statement is true is a general proof that holds for all objects in the domain.
- A mathematician may search for a counterexample showing that an unproven statement is false or a proof showing that it is true

Erroneous Theorem

If n is an integer greater than 1, then $(1.1)^n < n^{10}$

$$(1.1)^{100} < 100^{10}$$
$$13780.61 < 100000000000000000000$$

The statement holds true until n = 686

$$(1.1)^{686} < 686^{10}$$
$$2.4 \, x \, 10^{28} < 2.3 \, x \, 10^{28}$$

When n = 686 the inequality is false

Counterexamples for conditional statements

- A counterexample must satisfy all the hypotheses and contradict the conclusion.
- For a conditional statement:

$$\boxed{\forall x \; (H(x) \rightarrow C(x))}$$

- A counterexample is a specific element d in the domain such that H(d) is true and C(d) is false.

- For a statement with more than one hypothesis, such as:

$$\forall x\ ((H_1(x) \land H_2(x)) \to C(x))$$

- A counterexample must satisfy all the hypotheses and contradict the conclusion.

Erroneous Statement

For any real number x, if $x \geq 0$ and $x < 1$, then $x^2 < x$.

Hypothesis

$H_1(x) = x \geq 0$

$H_2(x) = x < 1$

Conclusion

$C(x) = x^2 < x$

Universal statement

$\forall x\ ((H_1(x) \land H_2(x)) \to C(x))$

Invalid Counterexamples

$x = 2$

- results in a false conclusion
- satisfies $H_1(x)$
- does not satisfy $H_2(x)$

$x = -1$

- results in a false conclusion
- does not satisfy $H_1(x)$
- satifies $H_2(x)$

Valid Counterexample

$x = 0$

- results in a false conclusion
- satisfies $H_1(x)$
- satisfies $H_2(x)$

Proving existential statements

- An existence proof shows that an existential statement is true.
- The most common type of existence proof is a constructive proof of existence.

- An existential statement asserts that there is at least one element in a domain that has some particular properties.
- A constructive proof of existence gives a specific example of an element in the domain or a set of directions to construct an element in the domain that has the required properties.

Example 1

Theorem: There is an integer that can be written as the sum of the squares of two positive integers in two different ways.

Proof:

Let $n = 50$

$50 = 1^2 + 7^2 = 5^2 + 5^2$

Therefore the integer 50 can be written as the sum of the squares of two positive integers in two different ways. ■

Example 2

Theorem: For every integer x, there is an integer y such that $y + 3 = x$

Proof:

Suppose that x is an integer.

Let $y = x - 3$.

Since x is an integer, $x - 3$ is also an integer.

Therefore y is an integer.

Furthermore $y + 3 = (x - 3) + 3 = x$. ■

Types of Existence Proofs

- Existence proofs can be constructive or nonconstructive.
- A constructive existence proof gives a specific example or set of directions to construct an element in the domain that has the required properties.
- A nonconstructive existence proof proves that an element with the required properties exists without giving a specific example.
- A common method for giving a nonconstructive existence proof is to show that the non-existence of an element with the required properties leads to a contradiction.

Disproving Existential Statements

- An existential statement asserts that there is at least one element in a domain that has some particular properties.
- To show that an existential statement is false, it is necessary to argue that every single element of the domain does not have the required properties.
- De Morgan's law says that the statement "It is not true that there exists an element x in the domain with property P" is equivalent to the statement "Every element x in the domain does not have property P."
- Therefore, the approach to proving that an existential statement is false is the same as the approach to proving that a universal statement is true.

Example

Erroneous Statement
There is a real number whose square is negative.

Disproof
The square of every real number is greater than or equal to 0.

2.3 Best practices and common errors in proofs

Proof Steps and Assumptions

- Most mathematical proofs make use of other facts that are assumed to be true.

- The amount of detail provided in a proof depends on the intended audience.
- A proof written for advanced readers can skip small steps under the assumption that the reader can fill in the details on their own.
- Each step of a proof should apply at most one rule of algebra at a time.
- It is important to provide a clear reference when using outside facts.

Allowed Assumptions in Proofs

The Rules of Algebra

The rules of algebra are fundamental to mathematics and allow us to manipulate expressions and equations to reach a desired result. For example, if x, y, and z are real numbers and $x = y$, then $x + z = y + z$. This is because we can add the same value (z) to both sides of the equation without changing its truth.

Closure of Integers

The set of integers is closed under addition, multiplication, and subtraction. In other words, sums, products, and differences of integers are also integers. For example, $2 + 3 = 5$, $2 \times 3 = 6$, and $2 - 3 = -1$, all of which are integers.

Even and Odd Integers

Every integer is either even or odd. This fact is proven elsewhere in the material. An even integer can be expressed as $2k$, where k is an integer, and an odd integer can be expressed as $2k + 1$, where k is an integer. Therefore, every integer can be classified as either even or odd.

Integers and Intervals

If x is an integer, there is no integer between x and $x+1$. In particular, there is no integer between 0 and 1. This can be shown using the definition of consecutive integers.

Ordering of Real Numbers

The relative order of any two real numbers can be determined using the symbols "<", ">", or "=" to denote which number is smaller, larger, or equal, respectively. For example, $1/2 < 1$ and $4.2 \geq 3.7$.

Squares of Real Numbers

The square of any real number is greater than or equal to 0. This fact is proven in a later exercise. For any real number x, x^2 is always greater than or equal to 0. This can be proven by cases: if x is positive, then x^2 is positive; if x is zero, then x^2 is zero; and if x is negative, then x^2 is positive.

Mathematical Proof Writing Tips

- Every step in a proof requires justification
- The reader needs to know if an assertion follows from an assumption of the proof, a definition, or a previously proven fact
- Proofs can vary in notation or word choice

Keywords and Phrases in Mathematical Proofs

"Thus" and "Therefore"

A statement that follows from the previous statement or previous few statements can be started with "Thus" or "Therefore".

- n and m are integers. Therefore, $n + m$ is also an integer.
- n is a positive integer. Thus, $n \geq 1$.

Other words that serve the same purpose are "it follows that", "then", "hence".

"Let"

New variable names are often introduced with the word "let".
For example, "Let x be a positive integer".

"Suppose"

The word "suppose" can also be used to introduce a new variable.
For example: "Suppose that x is a positive integer".

Suppose is also used to introduce a new assumption, as in: "Suppose that x is odd", assuming that x has already been introduced as an integer earlier in the proof.

"Since"

If a statement depends on a fact that appeared earlier in the proof or in the assumptions of the theorem, it can be helpful to remind the reader of that fact before the statement. The phrase "because we know that" can serve the same purpose.

For example, assuming that the facts $x > 0$ and $y > z$ have been established earlier, a proof could say:

- "Since $x > 0$ and $y > z$, then $xy > xz$."
- "Because we know that $x > 0$ and $y > z$, then $xy > xz$."

"By definition"

A fact that is known because of a definition, can be started with the phrase "By definition".
For example: "The integer m is even. By definition, $m = 2k$ for some integer k."

"By assumption"

A fact that is known because of an assumption, can be started with the phrase "By assumption".
For example: "By assumption, x is positive. Therefore $x > 0$."

"In other words"

Sometimes it is useful to rephrase a statement in a more specific way. The phrase "in other words" is useful in this context.

For example: "We must show that the average of x and y is positive. In other words, we must show that $(x+y)/2 > 0$."

"Gives" and "Yields"

Sometimes a proof is clearer if even an algebraic step is justified. The words "gives" and "yields" are useful to say that one equation or inequality follows from another.

- Multiplying both sides of the inequality $x > y$ by 2 gives $2x > 2y$
- Substituting $m = 2k$ into m2 yields (2k)2
- Since $z > 0$, we can multiply both sides of the inequality $x > y$ by z to get $xz > yz$

Best Practices in Writing Proofs

Indicate the Beginning and End of the Proof

- Clearly indicate where the proof begins and ends
- Typically, the proof starts with the word "Proof:" and ends with the symbol "■"

Write in Complete Sentences

- Write the proof in complete sentences, with mathematical expressions naturally incorporated as part of the sentence
- Use proper grammar and punctuation

Provide a Roadmap

- Give the reader an overview of what has been established, what assumptions are made, and where the proof is headed
- At the beginning of a proof, state what assumptions are being made and what will be proven
- In longer proofs, provide a summary of what has been proven so far and what still needs to be proven

Introduce Variables

- Introduce each variable when it is used for the first time
- Clearly specify the relationship between the new variable and the previously introduced variables or facts

Justify Each Step

- Justify each step of a proof with English text, indicating whether it follows from an assumption, definition, or previously proven fact
- Use proper notation and formatting
- If the justification for a step does not fit easily on the line of the equation, it can be provided immediately after the block of equations

Existential instantiation

- Existential instantiation is a law of logic that argues if an object exists, then it can be given a unique name.
- Names must not be currently used to denote something else.
- The definitions of odd and even numbers, rational numbers, and divides all use existential instantiation.

Example

If n is an odd integer, then n is equal to two times an integer plus 1.

That is, n = 2k+1, for some integer k

- Giving the integer k a name in $n = 2k + 1$ is an example of existential instantiation.

Common Mistakes in Proofs

When writing a proof, it is important to be careful and avoid making common logical errors. Here are some mistakes to watch out for:

Generalizing from Examples

To prove universal statements, one must either check every element in the domain or prove that the fact holds true for a generic element in the domain, despite the helpfulness of exploring specific examples.

- Evidence by example can provide valid examples and erroneous conclusions:

Bumble bees make honey,
and red ants will sting you.

∴ All bees make honey,
and all ants will sting you

- Evidence by example can also have valid conclusions:

m = 8 is an even integer since 8 = 2 · 4
$m^2 = 8^2 = 64$ is an even integer since 64 = 2 · 32

∴ if n is an even integer, then n^2 is also an even integer.

Skipping Steps

It is important to justify every step of a proof using allowed assumptions. It is an error to assume a fact is true without proving a reason.

If n is an odd integer, then $n = 2k+1$ for some integer k. $\therefore n^2 = (2k+1)^2$ and n^2 is odd.

- This proof omits important steps showing that the expansion of $(2k+1)^2$ is odd

Circular Reasoning

A proof that uses circular reasoning uses the fact to be proven in the proof itself.

If n is an odd integer, then $n = 2k+1$ for some integer k. Let $n^2 = 2j + 1$ for some integer j. Since n^2 is equal to two times an integer plus 1, then n^2 is odd.

- This proof jumps to the conclusion that n2 = 2j + 1 for some integer j. The fact that n2 is odd is the fact that needs to be proven.

Assuming Facts that Have Not Yet Been Proven

Every fact used in a proof must be previously proven and referenced or must be established within the proof.

Suppose r is a rational number. The product of any two rational numbers is rational. $\therefore r^2 = r \cdot r$ is also rational.

- The fact that the product of two rational numbers is rational has not been established in the proof and therefore cannot be used in the reasoning of the proof.

2.4 Writing direct proofs

Form of Direct Proofs

- A conditional statement in which a conclusion follows from a set of hypotheses is expressed as $p \to c$, where p is the hypothesis and c is the conclusion
- Direct proofs assume p is true and prove c as a direct result of the assumption
- Some theorems are conditional statements with a universal quantifier

> "For every integer n, if n is odd then n^2 is odd"
>
> D(n): n is an odd number
>
> $\forall n \, (D(n) \to D(n^2))$

- Direct proof of these theorems starts with an arbitrary object, typically using the variable of the quantifier, assumes the hypothesis, and then proves the conclusion
- Sometimes the universal quantifier and domain are expressed as part of the hypothesis, e.g. "If n is an odd integer, then n^2 is an odd integer"

Writing Direct Proofs

- After stating assumptions, a direct proof proceeds by proving the conclusion
- To begin the proof, name a generic object and state the assumptions about it
- Express any necessary facts using mathematical definitions or equations
- Use algebraic steps to show that the conclusion is true, typically leading toward an equation of a specific form
- The proof ends with a statement that the conclusion has been proven as claimed at the beginning

2.5 Proof by contrapositive

Introduction

- A proof by contrapositive proves a conditional theorem of the form $p \to c$ by showing that the contrapositive $\neg c \to \neg p$ is true.
- Many theorems are conditional statements that also have a universal quantifier such as:

> Theorem
>
> For every integer n, if n^2 is odd then n is odd.
>
> D(n): n is odd
>
> $\forall n\ (D(n^2) \to D(n))$

- A proof by contrapositive of the theorem starts with n, an arbitrary integer, assumes that D(n) is false, and then proves that $D(n^2)$ is false.

Contrapositive Theorem
For every integer n, if n is not odd, then n^2 is not odd.

D(n): n is odd
$\forall n\ (\neg D(n) \rightarrow \neg D(n^2))$

Alternatively
For every integer n, if n is even then n^2 is even.

E(n): n is even
$\forall n\ (E(n) \rightarrow E(n^2))$

Proof

Assume that n is even.
By definition, there exists an integer k such that n = 2k.

$\therefore n^2$

$= (2k)^2$

$= 4k^2$

$= 2(\ 2k^2\ )$

$= 2(\ m\ )$ where $m = 2k^2$

It is known that 2k is an even number.

Since 2m has the form of 2k, and then must be even.

$\therefore$ n^2 must be an even number.

Because the contrapositive of $\forall n\ (D(n^2) \rightarrow D(n))$ is true,
$\forall n\ (D(n^2) \rightarrow D(n))$ must also be true. ■

- The proof implicitly uses the fact that every integer is even or odd, so if an integer is not even, then the integer is odd.

Example

Prove:

if 3n + 7 is an odd integer, then n is an even integer.

Proof by Contrapositive:

assume n is an odd integer

By definition, n = 2k + 1 for some integer k

$$
\begin{aligned}
\therefore \quad 3n + 7 &= 3(2k+1) + 7 && \text{substitute n} \\
&= 6k + 3 + 7 \\
&= 6k + 10 \\
&= 2(3k+5) \\
&= 2(m) && \text{where } m = 3k+5
\end{aligned}
$$

Since 2m has the form of an even integer,

$3n + 7$ must be an even integer. ■

Direct Proof vs. Proof by Contrapositive

- The decision on whether to use a direct proof or a proof by contrapositive depends on which assumption provides a more useful starting point.
- A direct proof assumes the hypothesis and derives the conclusion, while a proof by contrapositive assumes the negation of the conclusion and derives the negation of the hypothesis.
- A direct proof may not always be the easiest method, as it may lead to complicated expressions or calculations, while a proof by contrapositive may simplify the expressions and calculation

Theorem: For every integer x, if x^2 is even, then x is even.

Proof:

Let x be an integer that is odd.

If x is odd, it can be expressed as 2k + 1, for some integer k.
Since k is an integer, $2k^2 + 2k$ is also an integer.

$$\begin{aligned} \therefore\ x^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \\ &= 2(\ m\ ) + 1 \end{aligned}$$

Therefore x^2 can be expressed as 2m + 1,
where $m = 2k^2 + 2k$ is an integer.

$\therefore$ x^2 is odd. ■

Irrational Numbers and Proofs by Contrapositive

- An irrational number is a real number that is not rational, and every real number is either rational or irrational but not both.
- If x is not irrational, then x is rational.
- The theorem that for every positive real number r, if r is irrational, then $\sqrt{r}$ is irrational, can be proven using a proof by contrapositive.
- A direct proof of this theorem is difficult because the assumption that r is irrational does not provide a concrete expression for r to work from.
- A proof by contrapositive assumes that $\sqrt{r}$ is rational, which provides a useful expression for r (the ratio of two integers) that can be used to

Theorem:

for every positive real number r, if r is irrational,
then $\sqrt{r}$ is also irrational.

Contrapositive:

for every positive real number r, if r is rational,
then $\sqrt{r}$ is also rational.

Known:

1. $r = \frac{a}{b}$, where a and b are integers, and b $\neq 0$.

2. Since r is a positive real number, $\sqrt{r}$ is also a positive real number.

3. Since r is not irrational, $\sqrt{r}$ must be rational.

$$\sqrt{r} = \frac{a}{b}$$

$$(\sqrt{r})^2 = (\frac{a}{b})^2 \qquad \text{square both sides}$$

$$r = \frac{a^2}{b^2}$$

Since a and b are both integers, $a^2 \ and \ b^2$ are both integers.

$\therefore$ r is equal to the ratio of two integers with a non-zero denominator, and r is not irrational. ■

Proofs by Contrapositive of Conditional Statements with Multiple Hypotheses

- In a proof by contrapositive, it is only necessary to show that one of the hypotheses is false.

Theorem
If H_1 and H_2 are both true then C is true.

$(H_1 \wedge H_2) \rightarrow C$

Contrapositive
If C is false, then H_1 or H_2 cannot both be true.

$\neg C \rightarrow (\neg H_1 \vee \neg H_2)$

Alternatively
If C is false and H_1 is true, then H_2 is false.

$(\neg C \wedge H_1) \rightarrow \neg H_2$

2.6 Proof by contradiction

Introduction

A proof by contradiction assumes the opposite of the theorem and demonstrates a logical inconsistency, proving the theorem true.

- Assumes theorem is false
- Leads to a contradictory conclusion: $r \wedge \neg r$
- Indirect proof
- Starts with "Suppose ¬t", where ¬t is the negation of the theorem

Prove:

For every pair of positive real numbers, a and b:

$$\sqrt{a} + \sqrt{b} \neq \sqrt{a+b}$$

Proof:

Suppose there are two real numbers, a and b, such that:

$$\text{a} > 0,\ \ \text{b} > 0\ \ \text{and}\ \ \sqrt{a} + \sqrt{b} = \sqrt{(a+b)}$$

$\therefore$

$$(\sqrt{a} + \sqrt{b})^2 = (\sqrt{(a+b)})^2$$

$$(\sqrt{a})^2 + 2\sqrt{(ab)} + (\sqrt{b})^2 = a + b$$

$$a + 2\sqrt{(ab)} + b = a + b$$

$$2\sqrt{(ab)} = 0$$

$$\sqrt{(ab)} = 0$$

$$ab = 0$$

$\therefore$ Since ab $= 0$, then a $= 0$ or b $= 0$

This is inconsistent with the fact that a > 0 and b > 0. $\blacksquare$

Proof by Contradiction and Proof by Contrapositive

- Both ways to prove something is true by assuming it's false and showing that's impossible
- Proof by Contrapositive is for "if this, then that" statements.
- Assumes "that" is false and shows "this" must also be false.
- Proof by Contrapositive is a special kind of Proof by Contradiction

A Classic Proof by Contradiction

Prove:

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

$\therefore$ Bird culture. ■

2.7 Proof by cases

- Useful for proving universal statements of the form ∀x P(x) for large domains
- Breaks down the domain of x into different classes where each class can be proven separately
- Each class is called a case
- Every value in the domain must be included in at least one case
- Cases are numbered and each case starts with "Case n:", where n is the case number
- Each case has its own set of assumptions and proofs

Prove:

For every integer x, $x^2 - x$ is an even integer.

$\therefore$ Bird culture. ■

Proof by Cases and the Absolute Value Function

- The absolute value of a real number x is defined to be $|x| = -x$ if $x < 0$, and $|x| = x$ if $x \geq 0$.
- Proof by cases is an acceptable method where a situation can be included in more than one case.
- When using the absolute value function in a proof by cases, it is important to consider both the positive and negative cases, and to ensure all situations are covered.

Prove:

For any real number x, $|x+5| - x > 1$

Case 1:
Case 2:

$\therefore$ Bird culture. $\blacksquare$

Without Loss of Generality

- Used in mathematical proofs to narrow the scope of a proof to one special case
- Often used when two cases are so similar that it is repetitive to include both
- The proof can be easily adapted to apply to the general case
- Sometimes abbreviated as WLOG or w.l.o.g.

Theorem:

For any two integers x and y, if x is even or y is even, then xy is even.

Without loss of generality, assume that x is even.
Then x = 2k for some integer k.
Plugging in the expression 2k for x in xy gives xy = 2ky = 2(ky).
Since k and y are integers, ky is also an integer.
Since xy is equal to two times an integer. $\blacksquare$

- Two cases can be used to prove the theorem: x is even and y is odd, or x is odd and y is even.
- The two cases cover all possibilities since the theorem assumes that at least one of x or y is even.
- The proofs for the two cases would be identical except for the roles of x and y being reversed.
- Alternatively, a proof could address only one case and use the term "without loss of generality".

Additional Proofs

Sum of a Positive Rational Number and its Inverse is ≧ 2

Theorem: if x and y are positive real numbers, then:

$$\frac{x}{y} + \frac{y}{x} \geqq 2$$

Proof:

The square of any real number is greater than or equal to 0.

$(x-y)^2 \geqq 0$	known
$x^2 - 2xy + y^2 \geqq 0$	expanded binomial
$\frac{x}{y} - 2 + \frac{y}{x} \geqq 0$	divided by xy
$\frac{x}{y} + \frac{y}{x} \geqq 2$	■

The Square of an Odd Number is Odd

Theorem: the square of every odd integer is also odd

1. Let n be an odd integer
2. By definition, there exists an integer k such that $n = 2k + 1$
3. By definition, there exists an integer m such that $m = 2k^2 + 2k$

$$\begin{aligned} n^2 &= (2k+1)^2 && \text{Substitute } n \text{ with } 2k+1 \\ &= 4k^2 + 4k + 1 && \text{Expand the binomial} \\ &= 2(2k^2 + 2k) + 1 && \text{Factor out the 2} \\ &= 2m + 1 && \text{Replace } 2k^2 + 2k \text{ with } m \end{aligned}$$

4. It is known that $2k + 1$ must be an odd number

$$\therefore \quad n^2 = 2m + 1 \text{ must be an odd number. } \blacksquare$$

The Sum of Two Rational Numbers is Rational

Prove:
If r and s are rational numbers, then r + s is a rational number.

Proof:
Since r and s are rational numbers,
$r = \frac{a}{b} \quad s = \frac{c}{d}$

Where a, b, c, and d are integers, and b and d are not equal to 0.

$$\begin{aligned} \therefore \quad r + s &= \frac{a}{b} + \frac{c}{d} \\ &= \frac{ad}{bd} + \frac{cb}{db} \\ &= \frac{(ad + cb)}{bd} \end{aligned}$$

1. Since a, b, c, and d are integers, it follows that (ad + cd) and bd must also be integers.

2. Since b and d cannot be zero, bd cannot be zero.

3. r + s is equal to the ratio of two integers.

$\therefore \quad r + s$ is a rational number. ■

Binomial Formula Proof

The binomial formula is a formula that provides a way to expand expressions of the form $(a+b)^n$, where n is a non-negative integer and a and b are any real or complex numbers.

Binomial Formula

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

where $\binom{n}{k}$ is the binomial coefficient, given by:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Usage

When n = 2:

$$(a+b)^2 = \binom{2}{0} a^2 b^0 + \binom{2}{1} a^1 b^1 + \binom{2}{2} a^0 b^2$$

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

Related Formulas

Combinations

$$\binom{n}{r} = \frac{n!}{r\,!(n-r)!}$$

$$\boxed{\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{120}{6(2)} = 10}$$

n choose r,
where n is the number of items in a set of distinct members,
and where r is the number of items chosen

Proof

1. Within the domain of the set of natural numbers, a binomial raised to the n^{th}power can be expressed as the sum of n + 1 expressions.

Let a, b, n $\in \mathbb{N}$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

- Note that binomial coefficients are represented by the $\binom{n}{k}$ expression.

2. The formula can then be expanded

$$= \binom{n}{0} a^n b^0 + \binom{n}{1} a^{n-1} b^1 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + \binom{n}{n} a^0 b^n$$

3. Each $\binom{n}{k}$ combination can be expressed in a factorial form

$$= \frac{n!}{(0)!(n-0)!} a^n b^0 + \frac{n!}{(1)!(n-1)!} a^{n-1} b^1 + \cdots + \frac{n!}{(n-1)!(1!)} a^1 b^{n-1} + \frac{n!}{(n)!(0)} a^0 b^n$$

4. Not finished...

What is this from?

This proof assumes that n = k + 1 and m ≧ 0

$$\begin{aligned} &\text{Plugging in } n = k+1 \text{ into } n^2 : \\ &\qquad n^2 = (k+1)^2 \\ &\qquad\quad = k^2 + 2k + 1 \\ &\qquad\quad \leq k^2 + 2k + 1 + m, \quad \text{because } m \geq 0. \end{aligned}$$