Direct Proof

MAT231

Transition to Higher Mathematics

Fall 2014

Outline

What is a proof?

One thing that high-school and college students often say they appreciate about mathematics is that "answers are either right or wrong."

What is a proof?

One thing that high-school and college students often say they appreciate about mathematics is that "answers are either right or wrong."

While this isn't always true, it is the case that a large part of mathematics is focused on knowing if something is *always* true, *sometimes* true, or *never* true. This knowledge is without ambiguity—we can know it for certain.

What is a proof?

The **proof** of a proposition is an argument that will convince any reader with suitable background that the proposition is always true.

What is a proof?

The **proof** of a proposition is an argument that will convince any reader with suitable background that the proposition is always true.

Mathematical proofs are often written in a formal style, but that is not required. Proofs can come in many different forms, but mathematicians writing proofs often strive for conciseness and clarity...

What is a proof?

The **proof** of a proposition is an argument that will convince any reader with suitable background that the proposition is always true.

Mathematical proofs are often written in a formal style, but that is not required. Proofs can come in many different forms, but mathematicians writing proofs often strive for conciseness and clarity...

...well, at least they should be clear to other mathematicians. ☺

Theorems

Definition

A **theorem** is a statement that is true and has been proved to be true.

Not surprisingly, some theorems are more significant than others. Arithmetic, Algebra, and Calculus all have theorems named "The fundamental theorem of..." From arithmetic we have

Theorem (The Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be represented in exactly one way (apart from rearrangement) as a product of one or more primes.

Types of Theorems

Our text uses the term **proposition** to mean a statement which is true, but not important enough to be called a theorem. (In other contexts, a proposition can merely be a statement which is either true or false; at least until it is proved true).

A **lemma** is a theorem whose main purpose is to help prove a more substantial theorem.

A **corollary** to a theorem is a result that can be established easily once the theorem is proved.

The Chicken and Egg Problem

Proving a theorem often involves making deductions using the *rules of inference*. These deductions move us from some statement or statements known to be true to one or more new statements that we can know are true.

To use this approach, however, we need to start somewhere...

Our starting points will be *definitions* and *axioms* (also called *postulates*).

Definitions

We begin with some key definitions that we will use frequently.

Definition

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

Definition

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

Definition

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

As noted in our text, definitions are often worded to sound like an implication (if-then), but really they should be treated like a biconditional (if-and-only-if).

Closure

Definition

Let S be a set of numbers. S is **closed under addition** if the sum of any two elements in S is a member of S.

Similar definitions exist for closure under subtraction, multiplication, and division.

- $\mathbb{N}$ is closed under what operations?

Closure

Definition

Let S be a set of numbers. S is **closed under addition** if the sum of any two elements in S is a member of S.

Similar definitions exist for closure under subtraction, multiplication, and division.

- $\mathbb{N}$ is closed under what operations? addition and multiplication, but not subtraction or division.
- $\mathbb{Z}$ is closed under what operations?

Closure

Definition

Let S be a set of numbers. S is **closed under addition** if the sum of any two elements in S is a member of S.

Similar definitions exist for closure under subtraction, multiplication, and division.

- $\mathbb{N}$ is closed under what operations? addition and multiplication, but not subtraction or division.
- $\mathbb{Z}$ is closed under what operations? addition, subtraction, and multiplication, but not division.
- $\mathbb{Q}$ is closed under what operations?

Closure

Definition

Let S be a set of numbers. S is **closed under addition** if the sum of any two elements in S is a member of S.

Similar definitions exist for closure under subtraction, multiplication, and division.

- $\mathbb{N}$ is closed under what operations? addition and multiplication, but not subtraction or division.
- $\mathbb{Z}$ is closed under what operations? addition, subtraction, and multiplication, but not division.
- $\mathbb{Q}$ is closed under what operations? all four, if we disallow division by zero.
- $\mathbb{R}$ is closed under what operations?

Closure

Definition

Let S be a set of numbers. S is **closed under addition** if the sum of any two elements in S is a member of S.

Similar definitions exist for closure under subtraction, multiplication, and division.

- $\mathbb{N}$ is closed under what operations? addition and multiplication, but not subtraction or division.
- $\mathbb{Z}$ is closed under what operations? addition, subtraction, and multiplication, but not division.
- $\mathbb{Q}$ is closed under what operations? all four, if we disallow division by zero.
- $\mathbb{R}$ is closed under what operations? all four, if we disallow division by zero.

Divisibility

Definition

Suppose a and b are integers. We say that a **divides** b, written $a|b$, if $b = ac$ for some $c \in \mathbb{Z}$. We say a is a **divisor** of b and b is a **multiple** of a. To say a does not divide b, we write $a \nmid b$.

Be careful; $a|b$ is not the same as a/b.

- $a|b$ is a statement that means a divides b; it is either true or false.
- a/b is a mathematical operation that yields a numerical result.
- Note that if $a|b$, then b/a is an integer.

Example

Finding the set of divisors of 10 means finding every a such that $a|10$. The set is $\{a : a|10\} = \{-10, -5, -2, -1, 1, 2, 5, 10\}$.

Prime Numbers

Definition

A natural number n is **prime** if it has exactly two positive divisors, 1 and n. An integer m is **composite** if it factors as $n = ab$ where $a, b > 1$.

Note:

- 1 is not prime because it has only one divisor, itself.
- 2 is the only even prime number.

Division Algorithm

Definition (The Division Algorithm)

Given integers a and d with $d > 0$, there exist unique integers q and r for which $a = dq + r$ and $0 \leq r < d$. We call d the **divisor**, q is the **quotient**, and r is the **remainder**.

Note: The remainder r is zero if $d|a$, otherwise it is a positive number strictly less than the divisor d.

If the division algorithm is applied to $56 \div 20$, we have

$$56 = 20 \cdot 2 + 16$$

so the quotient is 2 and the remainder is 16.

Be careful with negative numbers! Remember the remainder must always be non-negative: $-31 \div 7$ gives $-31 = 7 \cdot (-5) + 4$.

GCD and LCM

Definition

The **greatest common divisor** (GCD) of integers a and b, denoted $\gcd(a, b)$, is the largest integer that divides both a and b. The **least common multiple** (LCM) of non-zero integers a and b, denoted $\text{lcm}(a, b)$, is the smallest positive integer that is a multiple of both a and b.

While the GCD of a and b is relative easy to find if the prime factorizations of both a and b are available. If not, one can use the *Euclidean Algorithm.*

Euclidean Algorithm to find the GCD

The Euclidean Algorithm is based upon the following lemma:

Lemma

Let $a = bq + r$ where a, b, q, and r are integers with $b > 0$, and $0 \leq r < b$. Then $\gcd(a, b) = \gcd(b, r)$.

Proof.

Suppose d divides both a and b. Then d divides bq and also divides $a - bq = r$. Thus, d divides both b and r.

Now suppose that d divides b and r. Then d also divides $bq + r = a$ and so d divides both a and b.

Since every divisor of a and b is also a divisor of b and r and vice versa, the sets of divisors for these two pairs are identical and the must share the same greatest value. Therefore $\gcd(a, b) = \gcd(b, r)$. □

Euclidean Algorithm to find the GCD

Lets use the Euclidean Algorithm to find $\gcd(38, 22)$. The colors show how the numbers move from one line to the next based on the lemma we just proved.

$$\begin{array}{rcrcrcr} a & = & b & \cdot & q & + & r \\ \hline \end{array}$$

Euclidean Algorithm to find the GCD

Lets use the Euclidean Algorithm to find $\gcd(38, 22)$. The colors show how the numbers move from one line to the next based on the lemma we just proved.

a	$=$	b	$\cdot$	q	$+$	r
38	$=$	22	$\cdot$	1	$+$	16

Euclidean Algorithm to find the GCD

Lets use the Euclidean Algorithm to find $\gcd(38, 22)$. The colors show how the numbers move from one line to the next based on the lemma we just proved.

a	$=$	b	$\cdot$	q	$+$	r
38	$=$	22	$\cdot$	1	$+$	16
22	$=$	16	$\cdot$	1	$+$	6

Euclidean Algorithm to find the GCD

Lets use the Euclidean Algorithm to find $\gcd(38, 22)$. The colors show how the numbers move from one line to the next based on the lemma we just proved.

a	$=$	b	$\cdot$	q	$+$	r
38	$=$	22	$\cdot$	1	$+$	16
22	$=$	16	$\cdot$	1	$+$	6
16	$=$	6	$\cdot$	2	$+$	4

Euclidean Algorithm to find the GCD

Lets use the Euclidean Algorithm to find $\gcd(38, 22)$. The colors show how the numbers move from one line to the next based on the lemma we just proved.

a	$=$	b	$\cdot$	q	$+$	r
38	$=$	22	$\cdot$	1	$+$	16
22	$=$	16	$\cdot$	1	$+$	6
16	$=$	6	$\cdot$	2	$+$	4
6	$=$	4	$\cdot$	1	$+$	2

Euclidean Algorithm to find the GCD

Lets use the Euclidean Algorithm to find $\gcd(38, 22)$. The colors show how the numbers move from one line to the next based on the lemma we just proved.

a	$=$	b	$\cdot$	q	$+$	r
38	$=$	22	$\cdot$	1	$+$	16
22	$=$	16	$\cdot$	1	$+$	6
16	$=$	6	$\cdot$	2	$+$	4
6	$=$	4	$\cdot$	1	$+$	2
4	$=$	2	$\cdot$	2	$+$	0

Euclidean Algorithm to find the GCD

Lets use the Euclidean Algorithm to find gcd(38, 22). The colors show how the numbers move from one line to the next based on the lemma we just proved.

a	$=$	b	$\cdot$	q	$+$	r
38	$=$	22	$\cdot$	1	$+$	16
22	$=$	16	$\cdot$	1	$+$	6
16	$=$	6	$\cdot$	2	$+$	4
6	$=$	4	$\cdot$	1	$+$	2
4	$=$	2	$\cdot$	2	$+$	0

The last non-zero remainder 2 is the GCD of both 2 and 4. By our lemma it is also the GCD of 4 and 6, and of 6 and 16, etc., all the way back to our original pair 38 and 22.

Direct Proof

During our study of proofs, we will use several approaches. The most straight forward, called **direct proof**, proves the a proposition in the form

$$\text{If } P, \text{ then } Q$$

by assuming P (called the **hypothesis**) is true and, through a sequence of logical deductions, shows that Q (the **conclusion**) must be true.

Some hints:

- Be sure you are convinced the proposition you are trying to prove seems true. Try some examples and look for patterns you can exploit.
- Be sure you know what the conclusion should be. Think of proofs as like doing a problem where you know what the answer should be – you are trying to work toward it. In a very real sense you're trying to build a bridge from the hypothesis to the conclusion.

Direct Proof Example 1

Proposition

The sum of an even integer and an odd integer is odd.

Some things to consider:

- First question: do we believe this proposition? $2 + 3 = 5$, $28 + 437 = 465$, $-120 + 35 = 85$ all confirm the proposition. ✓

Direct Proof Example 1

Proposition

The sum of an even integer and an odd integer is odd.

Some things to consider:

- First question: do we believe this proposition? $2 + 3 = 5$, $28 + 437 = 465$, $-120 + 35 = 85$ all confirm the proposition. ✓
- It may be helpful to reword the proposition as an implication. Something like "If a is an even integer and b is an odd integer, then $a + b$ is odd."

Direct Proof Example 1

Proposition

The sum of an even integer and an odd integer is odd.

Some things to consider:

- First question: do we believe this proposition? $2 + 3 = 5$, $28 + 437 = 465$, $-120 + 35 = 85$ all confirm the proposition. ✓
- It may be helpful to reword the proposition as an implication. Something like "If a is an even integer and b is an odd integer, then $a + b$ is odd."
- We want to start with the hypothesis "a is an even integer and b is an odd integer" and work our way to the conclusion: $a + b$ is odd.

Direct Proof Example 1

Proposition

The sum of an even integer and an odd integer is odd.

Some things to consider:

- First question: do we believe this proposition? $2 + 3 = 5$, $28 + 437 = 465$, $-120 + 35 = 85$ all confirm the proposition. ✓
- It may be helpful to reword the proposition as an implication. Something like "If a is an even integer and b is an odd integer, then $a + b$ is odd."
- We want to start with the hypothesis "a is an even integer and b is an odd integer" and work our way to the conclusion: $a + b$ is odd.
- What does it mean for a to be even? From our definition, we know that $a = 2m$ for some integer m. Similarly, we know that if b is odd, then $b = 2n + 1$ for some integer n.

Direct Proof Example 1

Proposition

The sum of an even integer and an odd integer is odd.

Some things to consider:

- First question: do we believe this proposition? $2 + 3 = 5$, $28 + 437 = 465$, $-120 + 35 = 85$ all confirm the proposition. ✓
- It may be helpful to reword the proposition as an implication. Something like "If a is an even integer and b is an odd integer, then $a + b$ is odd."
- We want to start with the hypothesis "a is an even integer and b is an odd integer" and work our way to the conclusion: $a + b$ is odd.
- What does it mean for a to be even? From our definition, we know that $a = 2m$ for some integer m. Similarly, we know that if b is odd, then $b = 2n + 1$ for some integer n.
- We know the result we need: $a + b$ is odd. Working backward, we need to find that $a + b = 2c + 1$ for some integer c.

Direct Proof Example 1

Proposition

The sum of an even integer and an odd integer is odd.

Proof.

Suppose a is an even integer and b is an odd integer. Then, by our definitions of even and odd numbers, we know that integers m and n exist so that $a = 2m$ and $b = 2n + 1$. Then

$$a + b = (2m) + (2n + 1) = 2(m + n) + 1 = 2c + 1$$

where $c = m + n$ is an integer by the closure property of addition. We have shown that $a + b = 2c + 1$ for an integer c so $a + b$ must be odd. □

Direct Proof Example 2

Proposition

Suppose $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.

Direct Proof Example 2

Proposition

Suppose $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.

- Our strategy will be to work forward from the hypothesis **and** work backward from the conclusion, trying to link the ends of the argument together.
- We start with $a|b$ and $b|c$. This means that $b = am$ and $c = bn$ for some $m, n \in \mathbb{Z}$.
- Working backward from $a|c$, we have that $c = ak$ for some $k \in \mathbb{Z}$.

Direct Proof Example 2

Proposition

Suppose $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.

Direct Proof Example 2

Proposition

Suppose $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.

Proof.

Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$ then by the definition of divisibility there are integers m and n for which $b = am$ and $c = bn$. In this case

$$c = bn = (am)n = a(mn) = ak$$

where $k = mn$. Since c is a multiple of a, by the definition of divisibility we see that $a|c$. □

Proof by Cases

Sometimes it is not possible to construct a single "path" from hypothesis to conclusion.

In such cases we can use a **proof by cases**. Consider the following proposition:

Proposition

For any integer n, $n^2 + n$ is even.

- This could be restated as "If $n \in \mathbb{Z}$, then $n^2 + n$ is even."
- How can we start with an integer n and work to show $n^2 + n$ is even?
- We know we need to end up with $n^2 + n = 2q$ for some integer q, but how do we get there?

Proof by Cases

Sometimes it is not possible to construct a single "path" from hypothesis to conclusion.

In such cases we can use a **proof by cases**. Consider the following proposition:

Proposition

For any integer n, $n^2 + n$ is even.

- This could be restated as "If $n \in \mathbb{Z}$, then $n^2 + n$ is even."
- How can we start with an integer n and work to show $n^2 + n$ is even?
- We know we need to end up with $n^2 + n = 2q$ for some integer q, but how do we get there?

We'll try two cases: n even and then n odd.

Proof by Cases Example 1

Proposition

For any integer n, $n^2 + n$ is even.

Proof by Cases Example 1

Proposition

For any integer n, $n^2 + n$ is even.

Proof.

Suppose $n \in \mathbb{Z}$.

Case 1. If n is even we can write $n = 2q$ for some $q \in \mathbb{Z}$. In this case $n^2 + n = 4q^2 + 2q = 2(2q^2 + q)$ which, by definition, is even.

Case 2. If n is odd then $n = 2q + 1$ for some $q \in \mathbb{Z}$. Now $n^2 + n = (4q^2 + 4q + 1) + (2q + 1) = 2(2q^2 + 3q + 1)$ which is also even.

We find that $n^2 + 2$ is even when n is even and when n is odd. Therefore $n^2 + n$ must be even for any integer n. □

Proof by Cases Example 2

Proposition

Suppose $n \in \mathbb{Z}$. If n is not divisible by 3, then $n^2 + 2$ is divisible by 3.

Proof by Cases Example 2

Proposition

Suppose $n \in \mathbb{Z}$. If n is not divisible by 3, then $n^2 + 2$ is divisible by 3.

Proof.

Let $n \in \mathbb{Z}$ be given. By the Division Algorithm we can write $n = 3q + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < 3$. If $r = 0$ then $3|n$, so we consider the other two cases, $r = 1$ and $r = 2$.

Case 1. Suppose $r = 1$ so $n = 3q + 1$, which is not divisible by 3. However, $n^2 + 2 = 9q^2 + 6q + 3 = 3(3q^2 + 2q + 1)$, so $n^2 + 2$ is divisible by 3.

Case 2. Now suppose $r = 2$ so $n = 3q + 2$. As before, this is not divisible by 3. On the other hand, 3 does divide $n^2 + 2$ since $n^2 + 2 = 9q^2 + 12q + 4 + 2 = 3(3q^2 + 4q + 1)$.

Reviewing these cases, we see that whenever $3 \nmid n$, we find $3|(n^2 + 2)$, completing the proof. □

Proof Exercises

Write proofs for the following propositions.

1. If the integers m and n are both divisible by 3, then the number mn is divisible by 9.
2. Suppose $a, b \in \mathbb{Z}$. If $a|b$, then $a^2|b^2$.
3. Every perfect square is either a multiple of 4 or of the form $4q + 1$ for some integer q.
4. The sum of any two rational numbers is a rational number.