Week 8

Methods of Proving Theorems

Why??

Almost nothing in undergraduate, and some graduate, mathematics courses creates FEAR more than when an instructor announces that the students will be required to do proofs. Yet, we all prove statements frequently. To illustrate, we may be required to explain some fact to a child, a high school student, or a colleague. Our explanation is going to vary depending on what that person knows. When you have successfully explained the fact you have "proven it". All a proof is, is a logical, detailed explanation of why a statement is true. Our explanation will vary depending on to whom we are speaking. Just like there can be multiple correct directions for going from one location to another, there are often different proofs for the same mathematical statement.

In any course we take, we are always trying to improve our problem-solving abilities. In order to solve a problem, we must first make sure we have a clear idea of what the problem is, what the assumptions are (ie. the "givens"), and what we are trying to accomplish. This is precisely what we do in mathematical proofs. Spending some time thinking about proof techniques will enhance our problem solving abilities.

Another purpose of these notes is to help us to be able to read proofs contained in a textbook that we might be studying. Since a proof is a logical, detailed explanation of a statement, it helps to clear up any ambiguity we may have on the concept. It gets right to "the basics", the core definitions, of what we are studying. If we can read and understand a proof, we have mastered the key ideas of that concept. The ACM/IEEE recommendation on Discrete Structures recommends 12 lecture hours on proofs. In the material that follows I try to make the topic easy to follow.

Methods of Proving If … then … types of Theorems

All theorems in mathematics, or any application of mathematics, can be expressed as a "If … then …" statement(s). Therefore, the text and the notes below discuss methods of proving "If … then …" statements.

Example 1.

The distributive law for numbers is $a(b + c) = ab + ac$. It should really be stated in if . . . then . . . format as follows:
If a, b and c are any three real numbers **then,** $a(b + c) = ab + ac$.

Example 2.

Similarly, the commutative law for sets (under the operation of $\cup$) should be stated as:
If A and B are any two sets **then** $A \cup B = B \cup A$.

You should be able to take each of the logic and set laws given in the notes and write them in

"**If** … **then** …" format.

Before we proceed there are a few definitions that we need to know because they will be used in virtually all of our examples of proofs. It is important that you learn the definitions as given, not some alternate form of the definitions. They will be repeated again as we need them.

- Even integer: **An even integer is any integer that can be expressed in the form 2n for some integer n.**

- Odd integer: **An odd integer is any integer that can be expressed in the form 2n + 1 for some integer n.**

- Divides: **Let x and y be integers with x $\neq$ 0. We say that x divides y (notation x | y) if there exists an integer k such that y = kx.**

Some examples:
1) Is 6 an even integer?
Yes, 6 is an even integer since 6 = 2 times 3.

2) Is -8 an even integer?
Sure, since -8 = 2 times (some integer, namely, -4).

3) Is 0 an even integer?
Yes, because 0 = 2 (some integer, which is???).

4) Comments on the definition of Divides **.** **Note**: in elementary school, if we were asked whether 3 divides evenly into 15, we would think of $\frac{15}{3}$ = what number?

Since $\frac{15}{3}$ = 5, we would say yes, 3 divides 15. This gives us the above definition of Divides: 3 divides 15 because 15 = 3 x (the integer, 5). When you see x | y, think of $\frac{y}{x}$. That is, x divides evenly into y iff $\frac{y}{x}$ = k for some integer k.

The Direct Method of proof of P $\Rightarrow$ C Statements.

As we know from our discussions in logic "**If** P **then** C" statements or "P **implies** C" statements are frequently written in logical notation as P $\Rightarrow$ C.

Recall that P stands for the premise (or hypothesis) of the statement and C stands for the conclusion. The Direct Method of proof of P $\Rightarrow$ C statements is based on the definition of P $\Rightarrow$ C. Look at the two cases where P is true in the definition. If P is true then the complete statement P $\Rightarrow$ C is true when C is true. **So to prove a statement of the type P $\Rightarrow$ C true assume P is true and prove C is true. To do this start with P being true and end with C being true.**

This is called the **direct** method of proof of a $P \Rightarrow C$ statement. So, to use the **direct** method we start with the assumption P is true and we show that it (naturally) follows that C is true using axioms, definitions, previously established results, and rules of inference.

Format

Example 3.

Prove the following: If x is any even integer and if y is any even integer then xy is an even integer.

First, I will comment on some key ideas in proof techniques and then proceed with the proof.
Comments:

- Most proofs depend on basic definitions and concepts. Do not proceed any further until you truly understand these essential ideas. A major reason for wanting to prove something is because it will force us to learn these key concepts. (Certainly, people probably smarter than us did the proof of this statement many years ago.) In this example, the key definition is that of an even integer. What is the definition of an even integer? I am not asking what we think the definition may be but, what is **the** definition. We may have to look it up. Here is a form of the definition of even integer: **An even integer is any integer that can be expressed in the form 2n for some integer n.**
- Next do you truly understand the definition? Can you give some examples and explain them? For example, 6 is an even integer. Why? Is 0 an even integer? Why? (Answer: yes, because 0 = 2(0), that is, 0 can be written as 2 times an integer.)
- What method of proof will you try? Usually try the **direct** method first.
- What is the process for this method? What is the assumption, the premise? What are you trying to prove? Write the assumption(s) and the conclusion(s) out. This will focus you attention on what you are trying to do.
- Give reasons for each step in your proof. If you cannot give a reason for a particular step it is most likely wrong.
- Relax, with practice you will get most proofs most of the time.

Now I will repeat the statement and prove it. Before you look at my proof try one of your own.

The general format of a direct proof is:

Write out the **assumption**(s) and the **conclusion, then**

Start with P being true

DO STUFF

End with C is true

Example 3. (the proof):

If x is any even integer and if y is any even integer, then xy is an even integer.

Answer:

Proof: (Direct)

Assume x and y are even integers is true (**this is the premise, P)**. **Start** with this.
Next, write down specifically what you want to do. **To prove:** xy is an even integer is true**.** You want to prove that xy is an even integer, so you must show that xy can be expressed as 2 times some integer. **End** with this.

Start with P being true

x and y are even integers implies that x = 2n and y = 2m for some integers n and m. Why?

this implies that xy = (2n)(2m) Why?
this implies that xy = 2(2nm) Why?
this implies that xy is an even integer. Why? End with C is true
DONE.

Some people like to use logical notation so they would write the above as:

x and y are even integers $\Rightarrow$ x = 2n and y = 2m for some integers n and m. Why?
$\Rightarrow$ xy = (2n)(2m) Why?
$\Rightarrow$ xy = 2(2nm) Why?
$\Rightarrow$ xy is an even integer. Why?
DONE.

Example 4.

Prove the following: Let a, b, and c be integers.
If a | b and a | c, then a |(b + c).

Comments.

- The sentence "Let a, b, and c be integers" is just another way of saying let a, b, and c be any integers or for all integers a, b, and c. The statement we are trying to prove is "if a | b and a | c, then a |(b + c)". What is the premise? What is the conclusion?
- Before we begin, we need to understand what x | y means. Assume x and y are integers where $x \neq 0$. Read x | y as x "divides" y, which means x divides evenly into y, no remainder. So, 2 | 8 and 3 | 36 but 2 does not divide 5. Therefore, x | y means $\frac{y}{x}$ = some integer, say k, that is y = kx. A formal definition follows.
- **Definition:** Let x and y be integers with $x \neq 0$. We say that x divides y if there exists an integer k such that y = kx.

Look at the proof of example 5 and then do example 4.

Example 5.

Let a, b, and c be any integers (a not equal to 0). If a | b, then a | bc. (This is exercise 6 below).

First, I will outline the direct proof of this statement and then I'll repeat the outline and do the proof.

Proof: (Direct):

Assume: P is true, namely, a | b. Start here.

To prove: C is true, namely, a | bc End here

Outline:

Start a | b ⇒

⇒

⇒ **bc = a (some integer).** **How did I know to write this? See below in green.** *

⇒ a | bc **END**

Since this is the last step, then what is the most likely second last step? By definition of divides it is bc = a (some integer). I'll put this in the above and see if it helps me to get where I'm going.

Now I'll do the proof, that is, fill in the blanks in the above

Start a|b ⇒ b = ak for some integer k. This is the definition of "divides".
How can I go from here to the statement in red below? Simple just multiple both sides by c. to get

⇒ bc = (ak)c. OR bc = a(kc). Note: I've rearranged the terms a bit and used parentheses, ( ). Is it clear I have the form below so I'm done.

⇒ **bc = a (some integer).** *

⇒ a|bc **END**

- In the proof of example 5 there is a key point that I don't want you to miss. When doing proofs always write the start here step, the end step **and** the second last step whenever possible.

Example 6.

Let a, b, and c be integers. Then if a | b and a | c, then a |(b + c).

Try it yourself first like the outline above. What is the first step , the last, the second last? See red printing below.

Proof: (Direct)

Assume a | b and a | c is true.

To prove a |(b + c) (is true). That is, we want to prove that (b + c) = a • (some integer).

a | b and a | c ⇒ b = ak for some integer k and
c = al for some integer l. This is the definition of divides.

$\Rightarrow$	$b + c = ak + al$	Simply add both sides of the above equations.
$\Rightarrow$	$b + c = a(k + l)$	The distributive law.
$\Rightarrow$	$b + c = a$(some integer)	The sum of 2 integers is an integer.
$\Rightarrow$	$a \mid (b + c)$	This is the definition of divides.

So in summary the direct method of proof of P $\Rightarrow$ C Statements can be outlined the following way. All you have to do is know basic definitions and fill in the blanks as illustrated below.

Proof: (Direct)
Assume: P is true. Start here.
To prove: C is true End here

Outline:
Start P is true means

$\Rightarrow$

.

.

.

$\Rightarrow$ **Once you know the last step,** C is true, **you frequently can write the 2nd last step and maybe even the 3rd last step**

$\Rightarrow$ C is true **END**

Exercises:
Prove the following using the direct method of proof:

1. If x is any even integer and if y is any even integer then x + y is an even integer.
2. If x is any odd integer and if y is any odd integer then xy is an odd integer.
3. If n is an even integer then n^2 is an even integer.
4. If n is an odd integer then n^2 is an odd integer.
5. If n is an even positive integer then 7n + 4 is an even integer.
6. Let a, b, and c be any integers. If a | b, then a | bc.
7. Let a, b, and c be any integers. If a | b and b | c, then a | c.
8. Let a, b, and c be any integers . If ac | bc, then a | b.
9. If a is an odd integer then $8 \mid (a^2 - 1)$

The "Proof by Contradiction" method of proof of $P \Rightarrow C$ Statements.

An If … then ... (that is an $P \Rightarrow C$) statement is either true or false. If a $P \Rightarrow C$ statement is not false then it must be true. So if we assume that a $P \Rightarrow C$ statement is false and find that this cannot happen (get a contradiction) then the given $P \Rightarrow C$ statement must be true. In the following identity I will use the conventional $P \rightarrow C$ in place of $P \Rightarrow C$.

The **proof by contradiction** method of proof is based on the identity: $\neg[P \rightarrow C] \Leftrightarrow [P \wedge (\neg C)]$. How? To use the "proof by contradiction" method of a proof on a $P \Rightarrow C$ statement, we assume P is true, C is false, and prove that this gives a contradiction. Note: The usual place to start using this method is generally the false part of the "assumption" that C is false. Why?

Example 7.

Let n be an integer. Use the proof by contradiction method of proof to prove the following: "If $n^3 + 5$ is an odd integer then n is an even integer".

Answer:

So to prove a statement of the form $P \Rightarrow C$ using the proof by **contradiction method** the process is:

Assume (1) P is true and assume (2) C is false (note this is **2 different** assumptions) and then show that this gives a contradiction. The usual contradiction is to the assumption that P is true

So the outline of any proof by contradiction usually is:

START with C is false $\Rightarrow$

$\Rightarrow$

.

.

.

$\Rightarrow$ this contradicts the assumption that P is true

END

Now I will outline the proof of this example. To do so I must understand what C is (n is a even integer) and what P is ($n^3 + 5$ is an odd integer).

Proof: (by contradiction)

Assume n is even is false and also assume $n^3 + 5$ is odd is true and show that this gives a contradiction (the contradiction will most likely be to the assumption that $n^3 + 5$ is odd is true)

Outline:

Start n is even is false

$\Rightarrow$

.

.

$\Rightarrow$ $n^3 + 5 = 2$(some integer) **(c)**
$\Rightarrow$ $n^3 + 5$ is an even integer **(b)**
$\Rightarrow$ this contradicts the assumption that $n^3 + 5$ is odd is true **(a)**
END

NOTE I wrote the "start line" first then I knew what I wanted to prove, namely, line (a) so I wrote this at the bottom. For line (a) to be contradicted $n^3 + 5$ had to be even so line (b) had to occur so I wrote this down and for line (b) to happen line(c) had to happen.

Now I'll do the proof using the above outline

Start n is even is false
$\Rightarrow$ n is an odd integer

$\Rightarrow$ $n = 2x + 1$ for some integer x (definition of odd integer)

$\Rightarrow$ $n^3 + 5 = (2x + 1)^3 + 5$ (this is a key step. Line (b) tells me I want to talk about $n^3 + 5$ so I wrote what $n^3 + 5$ is)

$\Rightarrow$ $n^3 + 5 = 8x^3 + 12x^2 + 6x + 1 + 5$

$\Rightarrow$ $n^3 + 5 = 2(4x^3 + 6x^2 + 3x + 3)$

Note: I did this to get the above expression in the form of the next line (line (c)).
$\Rightarrow$ $n^3 + 5 = 2$(some integer) **(c)**
$\Rightarrow$ $n^3 + 5$ is an even integer **(b)**
$\Rightarrow$ this contradicts the assumption that $n^3 + 5$ is odd is true **(a)**
END

Now try to put reasons next to each step. The reason for step b is simply the definition of even integer. The reason for another step might be simply basic algebra.

Example 8.
Assume that n is an integer. Use the "proof by contradiction" method of proof to prove: "If $3n + 4$ is even then n is even".

Outline
Proof: (by contradiction)
Assume n is even is false and also assume $3n + 4$ is even is true and show that this gives a contradiction (the contradiction will most likely be to the assumption that $3n + 4$ is even is true)
Outline
Start n is even is false
$\Rightarrow$

.
.

$\Rightarrow$ 3n + 4 = 2(some integer) + 1 **(c)**
$\Rightarrow$ 3n + 4 is an odd integer **(b)**
$\Rightarrow$ this contradicts the assumption that 3n + 4 is even is true **(a)**
END

NOTE I wrote the "start line" first then I knew what I wanted to prove, namely, line (a) so I wrote this at the bottom. For line (a) to be contradicted 3n + 4 had to be odd so line (b) had to occur so I wrote this down and for line (b) to happen line(c) had to happen.

Can you fill in the steps to the above?

More exercises:
Use the proof by contradiction method of proof to prove the following:

1. If n^2 is an even integer then n is an even integer.
2. If n^2 is an odd integer then n is an odd integer.
3. If n is an integer and 3n + 2 is even then n is even.
4. If n is any integer and $n^3 + 7$ is odd then n is even.
5. If n^2 is not divisible by 3, then n is not divisible by 3.
6. If xy is an odd integer then (both) x and y are odd integers. Some hints for this one. When you assume that x and y are odd integers is false this means (by DeMorgan's law) that x is not odd or y is not odd, that is, x is even **or** y is even. So use three situations/cases.
   Case 1. x even, y odd, Case 2. x odd, y even and Case 3. x even and y even.
   In each case there is a contradiction to xy is odd.
7. If n is any integer then $n^2 - 4$ is not divisible by 4.

Warning if you are referring to other texts: The literature is a little confusing concerning the different "names of methods of proof". In some texts the **proof by contradiction** method is called the **indirect** method and the term indirect method means something else.

How to prove iff Theorems.

From the material in logic we know that "iff" means "if and only if" and the logical symbol, $\leftrightarrow$ or $\Leftrightarrow$ is often used in place of iff. From the chart *Common Implications and Equivalences* (text section 3.4, table 3.4.2), we know that $(p \leftrightarrow q) \Leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$ is a tautology, a statement, that is always true. In other words:
p iff q is equivalent to saying if p then q and if q then p or
p iff q is equivalent to saying if p then q and conversely.

That is, to prove an iff theorem one must prove two if … then … theorems.

In exercise 3 page 8 you proved: If n is an even integer then n^2 is an even integer and for exercise 1 page 11 you proved the converse of this statement namely, " If n^2 is an even integer then n is an even integer". The two statements combined could be expressed as: "n is an even integer iff n^2 is an even integer".

Example 9.

Prove: n is an even integer iff n^2 is an even integer.

Proof:

I will outline the proof. To do this I will state each part of the proof and skip enough space to do each part, so I will not forget each part.

I must prove two statements:
1. If n is an even integer then n^2 is an even integer (You proved this in exercise 3 page 8 using the direct method of proof) **AND**
2. If n^2 is an even integer then n is an even integer (You proved this part in exercise 1 page 11 using the proof by contradiction method of proof).

Note: sometimes both parts of an iff statement can be proved using the same method of proof and sometimes different methods must be used.

Example 10.

Let a and b be any two real numbers. Prove the following:
ab = 0 iff a = 0 or b = 0.

Proof:

We must prove the following two statements:
(a) If ab = 0 then a = 0 or b = 0
and
(b) If a = 0 or b = 0 then ab = 0.

To prove part (a) we use the direct method of proof.

Assume that ab = 0 and **prove** that a = 0 or b = 0. **To prove** a = 0 or b = 0 we need only show that one of the two parts of this or statement is true. Why? To do this assume that $a \neq 0$

show that when this happens b must be equal to 0. Why does this work? Since $a \neq 0$ then 1/a exists. Why? Now multiply both sides of ab = 0 by 1/a to obtain b = 0. This proves part (a).

To prove part (b) we use the direct method of proof.

Assume a = 0 or b = 0 **To prove** ab =0. Here we have to show that whether we assume that a = 0 or we assume that b = 0 the conclusion, ab =0 follows. So we have two cases/situations.

Case I.

Assume that a = 0 and prove that ab = 0. This follows from the definition of the multiplication of a number by 0 that we all learned in elementary algebra.

Case II.

Assume that b = 0 and prove that ab = 0. Again, this follows from the definition of the multiplication of a number by 0.

Here are some additional **exercises**.

1. n is an odd integer iff n^2 is an odd integer.
2. Let n be a positive integer. Prove: n is an odd integer iff $n^3 + 6$ is an odd integer.
3. Let n be a positive integer. Prove: n is odd iff 5n + 6 is odd.
4. Prove the following: The equation $ax^2 + bx + c = 0$ has a unique solution if and only if the discriminant $b^2 - 4ac = 0$. Hint. First express the iff statement as two if … then… statements and then prove each using the direct method of proof. For each if … then ... statement carefully write down your assumption and what you are trying to prove.
5. x is an odd integer iff $x^2 + 2x + 1$ is even

We close our discussion proof with a few "odds and ends" on proofs.

Proof by contraposition

Another valid method of proof is that where one proves the contrapositive. We know that the statement $(P \Rightarrow \mathbf{C}) \Leftrightarrow (\neg \mathbf{C} \Rightarrow \neg P)$ is a tautology. So for this method, instead of proving

$P \Rightarrow C$ true, we prove $\neg \mathbf{C} \Rightarrow \neg P$ true. Use the direct method of proof to do this. That is, assume $\neg C$ true and then prove that $\neg P$ is true.

How do we prove a statement is false?

Finally how does one show/prove that a statement is false? Consider the following sentence: "Every person taking this course is over six feet tall". To prove this statement is incorrect we need only show that there is at least one person taking the course who is **not** over six feet tall. This is called giving a **counterexample** (to the given statement). Look up this term in the index of the text for more examples.

Warning: (Counter) examples are used to prove theorems/statements false but examples **cannot** be used to prove theorems true.

Some "do's" and "don'ts" for proofs:

1. Always try the direct method of proof first. It usually works.
2. Always outline carefully what your assumptions are and what you are trying to prove. This will focus your attention on what you are given and where you are going.
3. Clearly specify the method of proof you are using, again this will focus your attention on the correct process.
4. Keep in mind that a proof is only a detailed explanation. If you don't understand what you have written then it is most likely wrong.
5. Above all else, RELAX; the worst that can happen is that you cannot complete the proof. That's OK, hopefully by writing down part of the proof you have focused you attention on the basic definitions and or concepts that you are studying.
6. If you are stuck partly through a proof, again that's OK; in fact, it is good to realize that you are stuck. Try another approach.