Lecture Notes : Week #2

Methods of Proof

Our goal this week is to understand what is required to prove a mathematical statement. We will develop three framework that will be able to use in order to prove such statements :

① Direct Method

② Contrapositive Method

③ Contradiction Method

We'll start with a definition.

DEF A proof of a mathematical statement is a logical argument which establishes the truth of a statement.

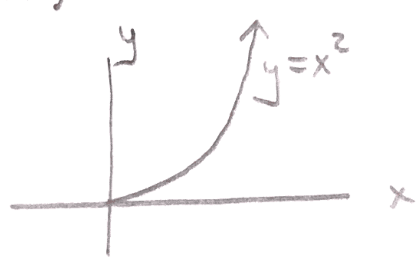
The mathematical statements we will be proving are conditional statements, precisely the same kind of statements we studied last week. The first thing we are going to do is work carefully through all that is required to show that a conditional statement is true. Consider the following:

<u>PROPOSITION</u> For positive real numbers a and b, if $a < b$, then $a^2 < b^2$.

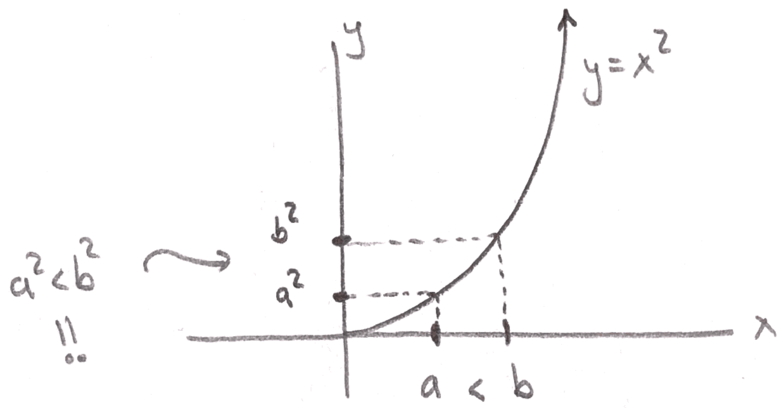
Take a moment and ask yourself this: does this statement seem true? If not, can you find a counterexample? (You won't be able to since the statement is actually true ...)

How might you explain *why* this statement is true to a friend or colleague?

This is one way I might try. Consider the following function: $y = x^2$. We know what this function looks like. This is how one could draw it (for positive x):



If we pick $x=a$ and $x=b$, where $a<b$, the shape of the graph appears to make a^2 be less than b^2.



And that would probably be good enough, right? It is reasonably convincing. But, I could ask several questions which might cast doubt:

1. What do I mean when I say the "Shape of the graph"?
2. Is the graph correct? The axes scales seem to be missing?
3. If I were to draw the correct graph (is that even possible?), would I be able to find a counterexample?

So here's the deal. The approach above might be a good way to share intuition, to help others understand the concept (or the underlying property that seems to be making the statement true). BUT, it is not a proof! In fact, and this is very important, (*) $\boxed{\text{pictures are not proofs}}$ (*).

Now, we could take this idea and turn it into a rigorous proof. We might want to define "increasing function" and then show that $y=x^2$ is increasing for positive real x. Maybe, if we defined "increasing function" correctly, we could show that increasing functions have the desired property: when $a<b$, $f(a)<f(b)$. Or, maybe we could leverage something more specific about the function $y=x^2$, such as its derivative, or concavity. Could we use calculus facts to rigorously prove the statement? Perhaps! But we are going to take a simpler approach. First, let's rephrase the statement so as to make its conditional nature completely clear:

PROPOSITION (Version 2)

If a, b are positive real numbers and $a < b$, then $a^2 < b^2$.

Notice:

Assumption / Hypothesis: a, b are positive real numbers **AND** $a < b$.
(Sufficient Condition!)

Conclusion: $a^2 < b^2$
(Necessary Condition!)

First, is this restatement really the same as our original proposition? (Yes! Convince yourself this is true.)

Next, let's consider one semi-weird thing ... Say $a = -3$ and $b = 2$. Is the statement false? Take a moment to think about this question.

continued on the next page.

So, you should be asking for a bit of clarification:

What do we mean by "statement"?

There is some ambiguity here: we could mean the <u>hypothesis</u>. If $a = -3$ and $b = 1$, then a is <u>not</u> positive, so "a, b positive real numbers <u>and</u> $a < b$" is a false statement. We can diagram it like this:

$$\underbrace{A}_{\text{the hypothesis } A \text{ is false.}} \Rightarrow B$$

However, if by statement, we mean the entire <u>conditional statement</u>, then the statement is still true!

$$A \Rightarrow B$$

A is false but $A \Rightarrow B$ is true!

If this feels jarring, check out the truth table for conditional statements in the lecture notes for week 1.

So here's the point:

Key Point

If we want to show that a conditional statement is true, we only need to worry about proving the conditional statement is true when the hypothesis is true, because if the hypothesis is false, the conditional statement is automatically true!

Hopefully, this, despite being a heavy "logic statement," jives with what you expected to be true. The only thing we need to do to show that a conditional statement is true is show it is true when the assumption is true.

This provides us with a logical framework for constructing proofs of a conditional statement:

1. Assume the hypothesis
2. Exhibit the conclusion as a logical consequence of the assumption.

this part requires some creativity

We summarize (and name this method) as follows.

Direct Method

To prove: $A \Rightarrow B$

Assume: A

Exhibit: B

Okay, well, let's give it a go.

Proposition: If a and b are positive real numbers and $a < b$, then $a^2 < b^2$.

Sketch of ideas:

What we know: $\begin{cases} \bullet\ a, b \text{ positive real numbers} \\ \bullet\ a < b \end{cases}$

Want to show: $a^2 < b^2$

We need to build a bridge from the assumption to what we want to show. To do this, we will use some basic arithmetic facts, or perhaps better said, a list of axioms that we all understand to be true. For example,

Axioms

1. For each pair of real numbers a, b, exactly one of these is true:

$$a<b, \quad a=b, \quad a>b$$

2. For real numbers a, b, and c,

$$a<b \iff a+c<b+c$$

3. For real numbers a, b, and c

$$a<b \iff ac<bc \quad \text{if } c>0$$

$$a<b \iff ac>bc \quad \text{if } c<0$$

4. For a, b, c real numbers

$$a<b \text{ and } b<c \Rightarrow a<c.$$

Back to the problem. With these axioms, can we bridge the gap between assumption and conclusion?

Observe: we want to go from $a<b$ to something with an a^2 and a b^2.

What might we do? Multiplying by a or b seems like a good choice. Let's try it.

$$a < b \text{, by hypothesis}$$

$$a \cdot a < a \cdot b$$

$$\longrightarrow a^2 < ab.$$

Ah! So it seems to work. BUT we need to explain why we can take each step:

$a < b$ $\boxed{\text{by hypothesis}}$ (*)

$aa < ab$, $\boxed{\text{since } a \text{ is positive and real,}}$ (*)
and Axiom 3!

so, $a^2 < ab$.

In other words, if $a < b$, then $a^2 < ab$.

Let's do the same, but now multiply by b:

$a < b$, $\boxed{\text{by hypothesis}}$ (*)

$ab < bb$, $\boxed{\text{since } b \text{ is a positive real number}}$ (*)
(and Axiom 3!)

so, $ab < b^2$.

Okay, so we have found two things so far.

$$① \quad a < b \implies a^2 < ab$$

AND

$$② \quad a < b \implies ab < b^2$$

In other words:

$$\boxed{a < b \implies a^2 < ab \text{ AND } ab < b^2}$$

Now, we are almost there. What does $a^2 < ab$ AND $ab < b^2$ really mean? It means $a^2 < ab < b^2$, i.e. it implies

$$a^2 < b^2,$$

yep, this is Axiom 4!

as desired. ☒

Great! We have a nice <u>sketch</u> of the proof. Unfortunately, however, if you turn that in for a homework proof, you won't get many points...

Why? In this class, you are expected to be able to

① Construct a proof (what we did!)

<u>and</u>

② Write them out carefully so that other people can understand them!

(*) Assume that when someone reads your proof, you are <u>not</u> there to help them understand what you wrote.

So, what should your proof look like? Fair question!

<u>proof</u>: Assume a and b are positive real numbers and that $a<b$. (*) Since a is positive, if we multiply $a<b$ by a on both sides, by Axiom 3, we get $a^2 < ab$. Similarly, * since b is positive *, if we multiply $a<b$ by b on both sides, by Axiom 3, we get $ab < b^2$. Thus, we see that $a^2 < ab$ and $ab < b^2$, in other words $a^2 < ab < b^2$, which implies $\boxed{a^2 < b^2}$, as desired. ☒

This is an important line! It tells your reader <u>HOW</u> you are proving the statement. Here, we are making it clear that we are using the <u>DIRECT METHOD</u> by stating our assumption.

This is absolutely required. You must show where you are using your assumptions!

nice touch, not necessarily required to point out when you use each axiom.

end with the <u>conclusion</u>!

For Homework #2:

For each proof you submit

① Submit your clean, well-written proof.
(Follow the structure of the example!)

② On a separate page (or pages), submit your sketch, i.e. scratch work.

Homework Question #1

Prove the following statement using the direct method.

If a, b are negative, real numbers and $a<b$, then $a^2>b^2$.

Homework Question #2

For this question, we will need a few definitions.

DEF An integer d divides an integer n if there is an integer m such that $n = dm$. If the integer d divides the integer n, we say that d is a divisor of n, n is divisible by d, and n is a multiple of d.

DEF Natural numbers greater than 1 whose only divisors among the natural numbers are themselves and 1 are called **primes**.

DEF An integer n is said to be **even** if 2 is a divisor of n. An integer n is said to be **odd** if it is not even.

Prove the following two statements, both using the direct method.

a) The only even prime is $n=2$.

b) If n is even, then n^3 is even.

Homework Question #3

Recall that the absolute value function is defined as follows:

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

Prove the following statement directly.

If c and a are prime numbers such that $c \neq a$, then $|c^3 - a^3| \geq 12$.

Hint: Show that $|c^3 - a^3| = |c-a| \cdot |c^2 + ca + a^2|$.

Let's continue now with a question. Since we are trying to prove that some conditional statement is true, could we modify the statement so that the new statement is logically equivalent, then prove the logically equivalent statement? Sure! In fact, we did this with the proposition and the second version of the proposition. Is there, perhaps, a more dramatic change we could make to a conditional statement without changing its meaning? We could take the contrapositive...

Remember:

$$A \Longrightarrow B \text{ is logically equivalent to}$$

$$\text{not } B \Longrightarrow \text{not } A, \text{ the contrapositive!}$$

So... instead of assuming "A", we could assume "not B":

<u>Assume:</u> not B

<u>Exhibit:</u> not A.

This is another logical framework that we can use!

Contrapositive Method

To prove: $A \Rightarrow B$

Assume: not B

Exhibit: not A

REMARK Notice that we haven't really done much. The contrapositive of $A \Rightarrow B$ is not $B \Rightarrow$ not A. If we apply the direct method to the statement not $B \Rightarrow$ not A, this is the contrapositive method of the statement $A \Rightarrow B$.

Now, there is an obvious question: Why would we choose this method over the direct method?

Occasionally, this method will be a bit easier to use than the direct method. Let's do a few examples and try to better explain why this is the case.

<u>THM</u> Suppose that m and b are real numbers with $m \neq 0$. Let f be a linear function defined by

$$f(x) = mx + b.$$

We can show:

If $x \neq y$, then $f(x) \neq f(y)$.

<u>Sketch</u> (Direct Method)

Assume $x \neq y$. Using basic arithmetic (which will be a part of the axioms we can use:

hypothesis

$$\boxed{x \neq y} \Rightarrow mx \neq my \quad \boxed{\text{for } m \neq 0 \quad (m \text{ real})}$$

Assumption

$$\Rightarrow mx + b \neq my + b \quad \boxed{\text{for } b \text{ real number}}$$

hypothesis

$$\Rightarrow f(x) \neq f(y), \quad \boxed{\text{by definition of } f(x)}$$

hypothesis

So we could write this up if we needed..

<u>Sketch</u> (Contrapositive Method)

First, let's find the contrapositive of "If $x \neq y$, then $f(x) \neq f(y)$."

It is:

"If $f(x) = f(y)$, then $x=y$."

(Check this!)

So now: Assume $f(x)=f(y)$ and deduce $x=y$.

$$\begin{aligned} f(x)=f(y) &\Rightarrow mx+b = my+b, && \text{definition of } f(x) \\ &\Rightarrow mx = my, && b \text{ is a real number} \\ &\Rightarrow x=y, && \text{by dividing by } m, \text{ since } m \neq 0. \end{aligned}$$

Notice: This is a bit cleaner. We don't have the "$\neq$", which really means "$>$ or $<$" by our inequality axioms. We should write that out carefully for a "direct method" proof.

REM This is not good enough to submit for HW. Instead, we could use this:

Here, we say assume $f(x)=f(y)$ to indicate to the reader that we are using the contrapositive method.

proof: $\boxed{\text{Assume } f(x)=f(y).}$ Then, by hypothesis, $mx+b=my+b$. Since b is a real number, we may subtract it from both sides yielding $mx=my$. Then, since m is real and $m\neq 0$, we can divide, implying $x=y$, as desired. ☒

Question: Was there an advantage to using the contrapositive?.

Maybe a little...

Let's try another.

THM Let a, b, c be integers such that $a > b$.

If $ac \leq bc$, then $c \leq 0$.

Sketch: (Direct Method) Let's try to compute ... see if we can start with $ac < bc$ to deduce $c \leq 0$...

$$ac \leq bc \implies ac - bc \leq 0$$

just means $ac - bc = 0$ or $ac - bc < 0$.

$$\implies (a-b)\,c \leq 0$$

So... either

① $a - b < 0$ and $c > 0$

OR

② $a - b > 0$ and $c < 0$

OR

③ $a - b = 0$ and $c = 0$

OR

④ $a - b = 0$

or

⑤ $c = 0$

Blegh. Is that all of them? We would need to carefully use the axioms to deduce all scenarios. Then, we would need to consider each scenario independently to see if it satisfies all assumptions, and if so, allows for $c<0$ or $c=0$.

For example, ① cannot happen: $a-b>0 \iff a>b$, but by hypothesis, $a<b$. Axiom 1 prohibits this!

Okay, so instead of finishing that sketch, let's try to use a different method.

Sketch: (Contrapositive Method)

What is the contrapositive of

"If $ac \leq bc$, then $c \leq 0$" ?

Negate and swap the implication:

Contrapositive: "If $c>0$, then $ac>bc$."

Already, this is looking cleaner.

Assume: $c>0$.

Now by Axiom 3, we know

$$a>b \iff ac>bc \quad \text{if } c>0.$$

Since $a>b$, $c>0$, we have $ac>bc$ immediately from this axiom! Thus, for $a>b$,

$$\boxed{\text{If } c>0, \text{ then } ac>bc.} \quad \blacksquare$$

Are we done? No! We need to write this out carefully:

Let's our reader know we are using the contrapositive method!

proof: Assume $c>0$. (Alternatively: The contrapositive of, "If $ac\leq bc$, then $c\leq 0$" is, "If $c>0$, then $ac>bc$." Assume $c>0$.)

(*) By hypothesis $a>b$, by axiom 3 we have that $ac>bc$, as desired. $\blacksquare$

This proof relies so heavily on Axiom 3 we really should cite it!

Okay, wow, the contrapositive method was much easier in that proof.

Moral: There are logical subtleties (and certainly a few arbitrary choices regarding exactly how we formulate the axioms - not the logical content of the axioms) which may mean that proving the contrapositive is easier than proving something directly! Try both!

Generally speaking, if you try one and the number of cases you need to consider continues to increase, see if the other method can help you reduce that number.

~~Homework~~ Question #4

Do not turn in, this will be a part of your next assignment!

Prove the following statement using the contrapositive method for both implications.

Let n be an integer. n^2 is odd if and only if n is odd.

Homework Question #5

Prove the following statement using the contrapositive method.

- Let a, b, c be integers.
- If a does not divide c, then either a doesn't divide b or b does not divide c.

Now let's develop one more logical framework that will help us prove statements. Occasionally, we may see statements like:

"There do not exist prime numbers a, b, c such that $a^3 + b^3 = c^3$."

Proving this via the "Direct Method" or "Contrapositive Method" may end up being hard.

<u>Why?</u> The statement is inherently negative, as in, it is asking us to show that something <u>never</u> occurs. Do we need to know everything that can occur in order to prove this? Hopefully not! That might be impossible ... or at the very least, extremely difficult.

So what can we do? Let's think about it. We are being asked to prove:

"If a, b, c are prime numbers, then $a^3 + b^3 \neq c^3$."

(i.e. "something" doesn't happen)

What if we assumed

$$\boxed{\begin{array}{l} \quad ① \ a, b, c \text{ are prime} \\ \text{AND} \\ \quad ② \ a^3 + b^3 = c^3 \end{array}} \quad ?$$

If the theorem is true, then there is something wrong with this assumption. In fact, if there is something wrong with this assumption, it would imply that the theorem (as a conditional statement) is true. (Check the old truth tables for conditional statements if you want.)

In other words, if we play with these two assumptions, we should find a logical inconsistency, i.e. a contradiction!

Contradiction Method

To prove: $A \Longrightarrow B$

Assume: A and not B

Exhibit: a contradiction!
i.e. a logical inconsistency!

Let's try this with a simple example first. We need a definition first.

<u>DEF</u> A real number r is <u>rational</u> provided there are integers m and n with $n \neq 0$ such that $r = \frac{m}{n}$.

A real number r is <u>irrational</u> if it is not rational.

<u>THM</u> $\sqrt{2}$ is irrational.

Let's rephrase that:

<u>THM</u> Let r be a real number. If $r^2 = 2$, then r is irrational.

<u>Sketch</u>: Assume: $r^2 = 2$ AND r is rational

Since r is rational, we can write

$$r = \frac{m}{n}.$$

We may as well assume m and n have no common divisors, otherwise we could divide them out.

Okay.. so what else are we assuming...

ah, $r^2=2$. So: $r=\frac{m}{n} \Rightarrow r^2=\frac{m^2}{n^2} \Rightarrow 2=\frac{m^2}{n^2}$.

So, we can write: $2n^2=m^2$.

Well, this doesn't seem to help much, but we can observe that since $2n^2=m^2$, we must have that m^2 is even.

Ah, by Homework Question 4, we can conclude that m must be even! (How?)

Thus, $m=2k$ for some integer k. That means:

$$2n^2=m^2=(2k)^2=4k^2$$

so, dividing through by 2, we see:

$$n^2=2k^2$$

In other words, n^2 is even, so n must be even! (why?)

Ah, but then both m and n are divisible by 2, which is a contradiction since we assumed that m and n had no common divisors, ☒

Homework Question #6

Carefully write out the proof of the theorem. Since you can use the sketch above, there is no need to submit your own sketch. Begin your prove with a line similar to: "Assume for the sake of contradiction that $r^2 = 2$ and r is rational." (Indicate to the reader that you are using the contradiction method.) End the proof after you exhibit the contradiction (with a line similar to: "Both m and n are divisible by 2 which is a contradiction since ... ").

Okay, let's try another one. Let's actually try the example we started with.

<u>THM</u> If a, b, c are prime numbers, then $a^3 + b^3 \neq c^3$.

Sketch:

Assume: • a, b, c are prime

AND

• $a^3 + b^3 = c^3$.

Notice, from our earlier homework problem, the only even prime is 2, so odds are that a, b, c are odd (no pun intended). Let's start with this...

If a and b are both odd, then a^3 and b^3 are odd by an earlier homework question. That means $a^3 + b^3$ is the sum of two odd integers. If you think about it, the sum of two odd integers is even (can you prove that with our earlier definition of odd and even?)

Assume that this is true for a moment. That would mean c^3 is even, and by an earlier homework problem, that implies c is even! i.e. $c = 2$. But that's nonsense, because $2^3 = 8$, and even if $b = a = 3$, $3^3 + 3^3 > 8$.

That is interesting. It means that both a and b cannot be odd, so at least one of them must be even.

$$a^3 + b^3 = c^3 \implies \overset{2^3}{\overset{\shortparallel}{8}} = c^3 - a^3$$

or

$$8 = c^3 - b^3.$$

Now, recall from an earlier homework problem, you discovered

$$(c^3 - a^3) = (c-a)(c^2 + ca + a^2),$$

and that

$$|c^3 - a^3| \geq 12.$$

This is a contradiction! We cannot have that both $8 = c^3 - a^3$ and $|c^3 - a^3| \geq 12$ since $c^3 - a^3 = 8 \implies |c^3 - a^3| = |8| = 8$. ☑

Homework Question #7

Prove by contradiction that the sum of two even integers is even. Start by restating the problem as a conditional statement of the form: "If ..., then ...."

~~Homework~~ Question #8 (Do not turn in! We'll come back to this one!)

Prove, by any method of your choosing, that the sum of two odd numbers is even.

(Be careful! Our definition of an odd integer is that it is not even.)