MATH 2406 Fall 2011

Our goals in this course are:

- To learn how to write a rigorous mathematical proof.
- To learn some serious abstract mathematics. (Topics are from abstract vector spaces, real analysis, group theory, ...).

There will be a great deal of writing and rewriting in this course. You will also be required to type the proofs for the homework problems (using a software program of your choice). LaTeX is recommended for this; some templates will be supplied with the first homework assignment.

©2013 Christopher Heil

1.1 Some Examples

Here is a sample theorem & proof. We will take some facts about numbers for granted while doing this proof, but usually we need to be very careful to only use facts that we have already proved.

Theorem A

$\sqrt{2}$ is irrational.

Proof (this is an example of a proof by contradiction).

Suppose that $\sqrt{2}$ was a rational number. By definition, this means that there are integers p and q such that

$$\sqrt{2} = \frac{p}{q}. \quad (1)$$

(This means that we are labelling this equation as equation #1)

We can assume that p & q have no integer factors other than 1 in common (if they do, we can just divide both p & q by that factor — we cancel it out, in other words). Another way to say this is that we can assume that the fraction p/q is in lowest terms.

Squaring both sides of equation (1), we see that

$$2 = \frac{p^2}{q^2},$$

and this implies that

$$p^2 = 2q^2. \qquad (2)$$

Hence p^2 is an even number.

Does the fact that p^2 is even tell us anything about the number p itself? [I wrote this sentence to give you some motivation, but we usually aren't quite so "conversational" in most proofs.]

Let's think about it. p must be either even or odd. Even means an integer multiple of 2, while odd means a multiple of 2 plus 1. Thus, if p is odd then

$$p = 2k+1 \quad \text{for some integer } k.$$

Squaring both sides of this equation, we see that in this case we have

$$p^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1.$$

Hence p^2 is one more than a multiple of 2, so p^2 is odd. Since we already saw that p^2 is even, this just can't happen — p cannot be odd.

we've shown that the "if" up here is impossible.

Since p isn't odd, it must be even. Hence, from knowing that p^2 is even, we have deduced that p itself must be even.

[Digression: It's not enough to argue by examples. 4, 16, 36, 64, 100 are all squares of even numbers, but there are infinitely many of these so you can't possibly check all of them if you try to do it one at a time.]

OK, what we know now is that p is an even number. This tells us that

$$p = 2n \quad \text{for some integer } n.$$

Hence $p^2 = 4n^2$. We also know from equation (2) that $p^2 = 2q^2$. Therefore

$$2q^2 = p^2 = 4n^2,$$

so by dividing by 2 it follows that

$$q^2 = 2n^2.$$

Thus q^2 is a multiple of 2, so q^2 is even.

Just as we showed for p^2, the fact that

q^2 is even implies that q is even. Therefore

$$q = 2m \text{ for some integer } m.$$

We have shown that there are integers m & n such that $p = 2n$ and $q = 2m$. But then p & q share an integer factor (other than 1), yet at the very beginning of the proof we said that we had divided p & q by any common factors.

Even though we started with p & q having no common factors, we have shown that they do share a common factor of 2. Our assumption that $\sqrt{2}$ is rational has led us to a contradiction. Hence that assumption cannot be true, which means that $\sqrt{2}$ is irrational. ▨

↑ "end of proof" symbol to show that the proof has been completed.

Note the little "subargument by contradiction" that we did in the middle of the proof – we showed that *if* p^2 is even & p is odd *then* there's a contradiction. This is just a little "local theorem" that tells us that "p^2 even + p odd" can't happen. Often we split the

little baby theorems off & state them separately as <u>lemmas</u> (small theorems used to prove another theorem).

For example, before stating the "$\sqrt{2}$ is irrational" theorem, it might have been nice to state (and prove) the following lemma first.

<u>Lemma B</u>

a. If n is an integer & n^2 is even, then n is even.

b. If n is an integer & n^2 is odd, then n is odd.

<u>Exercise</u> [I will state many "exercises" in the notes. I strongly suggest that you do all of these carefully. However, you do not have to hand in their solutions unless I specifically include on of these exercises on a formal homework assignment.]

Here is the exercise: Rewrite Theorem A and its proof so that it becomes a Lemma (with proof) and Theorem (with proof), like this.

Lemma B. (State the lemma)
Proof. (prove it.) ∎

Theorem A. (State the theorem)
Proof. (prove it, using Lemma B along the way) ∎

Some remarks

a. If you look at my proof of Theorem A, you will see that it is written IN ENGLISH.

Your proofs must likewise be written in English, in complete sentences, with proper grammar and correct spelling. Proofs that do not fulfill these requirements will receive zero credit.

Further, proofs on homework assignments must be typed.

b. Of course mathematical proofs will include symbols (often lots of them), but symbols are just shorthand for words. For example, "$a = b$" means "a is equal to b."

Only use symbols that we have defined in class or are so standard that there can be no confusion, such as:

$$=, \quad +, \quad -, \quad \sum_{k=1}^{\infty}, \quad \int_a^b$$

c. Some UNACCEPTABLE symbols:

$\therefore$, $\because$ ← Do not use these!

Exercises

1. Prove (carefully) that $\sqrt{3}$ is irrational.

2. Prove (carefully) that $\sqrt{5}$ is irrational.

Hints: Lemma B is useful for showing that $\sqrt{2}$ is irrational, but it's not much help with $\sqrt{3}$ or $\sqrt{5}$. You need to come up with a related but slightly different lemma.

3. Prove that if n is an even integer, then $n+1$ is odd, and if n is odd then $n+1$ is even.

Remark: We're taking the following for granted (i.e., this is our definition of even & odd):

n is even $\Leftrightarrow$ $n = 2k$ for some integer k
n is odd $\Leftrightarrow$ $n = 2k+1$ " " " "

4. Prove that the product of any two odd numbers is odd.

Definition

A real number r is <u>rational</u> if $r = \frac{m}{n}$ where m, n are integers & $n \neq 0$.

Exercises

a. Prove that the product of two rational numbers is rational.

b. Can you prove that the product of two irrational numbers is irrational?

WRITING PROOFS

Christopher Heil
Georgia Institute of Technology

A "theorem" is just a statement of fact. A "proof" of the theorem is a logical explanation of why the theorem is true.

Many theorems have this form:

Theorem I. *If statement A is true then statement B is true.*

This just means that whenever statement A is valid, then statement B *must* be valid as well. A proof is an explanation of WHY statement B must be true whenever statement A is true.

1. Direct Proofs.

There are several ways to write a proof of the theorem "If statement A is true then statement B is true." We'll discuss several of them in these pages. It may not be obvious at first which variety of proof to use, but a good rule of thumb is to try a *direct proof* first.

A direct proof. Start by assuming that statement A is true. After all, if statement A is false then there's nothing to worry about; it doesn't matter then whether B is true or false. So, suppose that statement A is true—write that down as the first step. This is information that you can use and build on. Now try to proceed logically, one step at a time, building on this information until you have shown that statement B is true.

An important point is that a proof is always written in *English*! There are mathematical symbols mixed in with the words, but you must write clear, complete, English sentences, one after another until you've made your way through to statement B. Finally, write an "end-of-proof" symbol like Q.E.D. or □ to show that you've finished the proof.

Here is an example of a simple theorem and a simple direct proof.

Theorem 1. *If p is a prime number bigger than 2, then p is odd.*

Proof. Suppose that p is a prime number and $p > 2$. *(That's where we've assumed that statement A is true. Now we build on this until we've shown that statement B is true.)* To show that p is odd, we have to show that p is not divisible by 2. Now, because p is a prime number, it is divisible only by 1 and itself. Since $2 \neq 1$ and $2 \neq p$, the number 2 is not one of the numbers that divides p. Therefore p is not divisible by 2, and hence p is an odd number. □

Admittedly, that was a pretty easy theorem and a pretty easy proof, which I've made excessively long just to give you the idea. Most theorems are harder, and you have to sit and think before you get the proof straight.

DON'T BE DISAPPOINTED IF YOU DON'T SEE HOW TO DO THE PROOF RIGHT AWAY! Most of the time, it takes THREE sheets of paper to write a proof:

© 2011 by Christopher Heil

Here is a final example of a proof by contradiction. This theorem was proved by Euclid a LONG time ago. Note that the statement of the theorem is slightly different than what we've discussed: it has the form "statement B is true" without any dependence on some statement A. All the same principles apply, however.

Theorem 3. (Euclid) *There are infinitely many prime numbers.*

Proof. Suppose that only finitely many prime numbers existed. *(Here is where we assume that statement B is false.)* Let's call these finitely many prime numbers $p_1, p_2, \ldots, p_N$. Now consider the number $m = p_1 p_2 \cdots p_N$, the product of all of those prime numbers. This number m is evenly divisible by each of $p_1, p_2, \ldots, p_N$. Therefore, by Theorem 2, $m + 1$ is NOT divisible by any of $p_1, p_2, \ldots, p_N$! Thus $m + 1$ is only evenly divisible by 1 and itself. But then $m + 1$ is a NEW prime number, bigger than any of $p_1, p_2, \ldots, p_N$. This is a contradiction, because we said that $p_1, p_2, \ldots, p_N$ were ALL the prime numbers that there were in the universe. Since we have obtained a contradiction, our assumption that there existed only finitely many prime numbers must be incorrect. Hence, there must be infinitely many prime numbers. □

It might surprise you learn that the existence of arbitrarily large prime numbers is of vital importance in cryptography. Governments—and businesses—are paying huge sums of money to encode data using schemes based on huge prime numbers. A fast factoring algorithm is the holy grail of much computing research!

Question: Look carefully at the proof of Euclid's theorem. Does that proof show that if $p_1, p_2, \ldots, p_N$ are prime numbers then $m = p_1 p_2 \cdots p_N + 1$ is also a prime number? Let's check:

$$\begin{aligned} 2 + 1 &= 3 \text{ is prime} \\ 2 \cdot 3 + 1 &= 7 \text{ is prime} \\ 2 \cdot 3 \cdot 5 + 1 &= 31 \text{ is prime} \\ 2 \cdot 3 \cdot 5 \cdot 7 + 1 &= 211 \text{ is prime} \\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 &= 2311 \text{ is prime} \\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 &= 30031 = 59 \cdot 509 \text{ is NOT prime!!} \end{aligned}$$

What went wrong? NOTHING! There's nothing wrong with the proof of Euclid's theorem. Just be careful about what it says. All that the proof says is that IF there were only finitely many prime numbers $p_1, p_2, \ldots, p_N$ THEN $m = p_1 p_2 \cdots p_N + 1$ would be prime. But we showed that there AREN'T finitely many prime numbers, so the statement "IF there were only finitely many prime numbers $p_1, p_2, \ldots, p_N$ THEN $m = p_1 p_2 \cdots p_N + 1$ would be prime" is vacuous, i.e., it simply doesn't apply.

4. If and Only If Theorems.

Here is another typical type of theorem:

Theorem III. *Statement A is true if and only if statement B is true.*

This is logically equivalent to two theorems:

Andy Miller
U. OK

Discrete Mathematics
Math 2513

Some Guidelines for Constructing and Writing Proofs

1. A proof really just consists of a sequence of sentences each of which follows from the preceding ones by common-sense logic incorporating references to definitions, hypotheses or previously proven theorems.

2. Before starting to organize the ideas for your proof make sure that you clearly understand the hypothesis (or hypotheses) and the conclusion of the statement to be proven. Determine all of the key definitions that play a role in the statement to be proven, and make sure you are familiar with these definitions before starting to construct your proof. Just thinking about the key definitions should start to give you ideas about how to construct your proof.

3. Do scratch work on the side to think out the line of explanation that you will use. Do this before starting to write your final proof. For more difficult proofs it is often necessary to do two or more rounds of scratch work before writing the final version. Your scratch work may incorporate Venn diagrams or other schematic diagrams, whatever helps you to organize the ideas.

4. In organizing your proof it's almost always good to start by examining the desired conclusion and thinking about what will need to be done to verify it. In other words, in your scratch work start at the end and work backwards.

5. Are there any previously proved theorems that you might use to shorten your proof?

6. Always keep the intended reader in mind when you are writing and try to make it easy for them to follow what you are doing. This can be difficult, but try to view your final written proof from the perspective of a reader who has not spent as much time thinking about the problem as you have.

7. Make sure that your final written proof starts with a complete statement of the result that you intend to prove. This is important so that both the reader and you will have a clear statement of the desired outcome.

8. If you are using unusual definitions are worry that the reader may not know or remember a key definition then provide a formal statement of the definition.

9. In your final proof, be sure to write in complete and grammatically correct sentences. Remember that a sentence starts with a capital letter and ends with a period. It has a verb, a subject and a predicate.

10. Use the first sentence or two of your proof to declare any variables that you will use. If there is some object that you will refer to frequently throughout the proof then you should consider introducing a variable for that object so that you can refer to it easily during the proof. After declaring variables, use the next sentence or two to write out the hypotheses of the statement you are proving.