ADVICE FOR STUDENTS FOR LEARNING PROOFS

You should periodically reread this essay as the course progresses since many of the comments refer to situations that will arise from time to time. Keep it on hand when you do home work.

Proofs are constructed by utilizing definitions, theorems and facts. So, to be able to do proofs you must have the relevant definitions, theorems and facts memorized. When a new topic is first introduced proofs typically use only definitions and basic math ideas such as properties of numbers. Once you have learned some theorems about a topic you can use them to proofs more theorems.

To learn how to do proofs pick out several statements with easy proofs that are given in the textbook. Write down the statements but not the proofs. Then see if you can prove them. Students often try to prove a statement without using the entire hypothesis. Keep in mind that you MUST use the hypothesis. If you cannot prove the statement, look at the first line of the proof in the text. That might be enough to get you started. If it is not, then look at the next line and so on. Practice proving the statements you selected until you can do the proofs without looking at the text. One you have mastered your original selections pick a few new ones and practice those. There is a direct relationship between your understanding of the subject and your ability to do proofs. Proofs test your understanding. They also test your creativity.

HOW TO GET STARTED

Begin a proof by rewriting what you are given and what you are asked to prove in a more convenient form. Often this involves converting word to symbols and utilizing the definitions of the terms used in the statements. An example is "Prove that the product of two nonzero real numbers is nonzero." This converts to "If a and b are nonzero real numbers, prove that $ab \neq 0$." Begin the proof with "Assume that $a \neq 0$ and $b \neq 0$. Prove that $ab \neq 0$." (We provide a proof of this statement in the section on proof by contradiction.) It is important to begin by rewriting both the assumptions and the conclusions since this emphasizes that the former is what you have to work with and the latter is your goal.

Examples of converting words to symbols are:
n is an even integer converts to $n = 2t$ for some t
n is an odd integer converts to $n = 2t + 1$ for some t

n is a rational number converts to $n = a/b$ where a and b are integers
n is a divisor of m converts to $m = nt$ for some integer t
n is a square converts to $n = t^2$ for some integer t.

DIRECT PROOF

In a direct proof you are given one or more conditions and are asked to prove some conclusion. For proofs in abstract algebra you are permitted to use the given conditions as well as axioms, definitions and standard facts about real numbers, complex numbers, high school algebra, and linear algebra without elaboration. In a direct proof of a statement of the form A implies B, you start your proof by assuming that A is true and go through a series of steps ending with B.

As an example, consider the statement "The sum of two rational numbers is rational." To prove this we use the definition of a rational number and convert the words to expressions by recasting the statement as "If a, b, c and d are integers and $b \neq 0$ and $d \neq 0$ are not 0, then $a/b + c/d$ has the form m/n where m and n are integers." To prove this statement we observe that since $a/b + c/d = (ad + bc)/bd$ and $ad + bc$ is an integer and $bd \neq 0$, the proof is complete.

PROOF BY CONTRADICTION

Proof by contradiction is a natural way to proceed when negating the conclusion gives you something concrete to manipulate. To prove the statement "A implies B" by contradiction, begin by assuming that A is true and B is not true and end by arriving at some contradiction (possibly contradicting statement A). For example, a statement such as "Prove that $\log_2 3$ is irrational" is an obvious choice for proof by contradiction since assuming that $\log_2 3$ is rational allows you to write $\log_2 3 = m/n$ where m and n are integers. From this we have $3 = 2^{m/n}$ and therefore $3^n = 2^m$. Since the right side is even and the left side is odd we have contradicted a basic fact about integers. If you argue by contradiction, don't end it by saying "a contradiction." You must indicate what you are contradicting (usually this will be the hypothesis, a theorem or a fact).

Here is an example where we contradict the original assumption. To prove the statement "The sum of a rational number and an irrational number is irrational" by contradiction, we let a be a rational number and b an irrational number and assume that $a + b$ is rational. But then $(a + b) + (-a) = b$ is rational. This is a contradiction to the assumption that b is irrational.

Over 2000 years ago Euclid proved that are infinitely many primes by assuming that there are only finitely many. By doing so he was able to take their product to arrive at a contradiction.

PROVING AN "OR" STATEMENT

When you are asked to prove an "or" statement such as "... prove statement A or statement B" you begin by assuming one of A or B is false and use that to prove the other statement is true. It does not matter which of the statements A or B you assume to be false. If you assume A is false and are not able to prove B is true, then assume B is false and try to prove that A is true. Proving one of these two possibilities is a complete proof. There is no need to do both.

Another way to prove an "A or B" statement is to assume both statement A and statement B are false and obtain a contradiction. The statement "If *a* and *b* are nonzero real numbers, prove that *ab* is nonzero" is a perfect candidate for proof by contradiction since the assumption that $ab = 0$ allows you to take advantage of a special property of 0. To prove $ab \neq 0$ we assume that $a \neq 0$, $b \neq 0$ and $ab = 0$. Since $b \neq 0$, we know b^{-1} exists. Then $a = a(bb^{-1}) = (ab)b^{-1} = 0$, which contradicts the assumption that $a \neq 0$.

Here is another example. "If *m* and *n* are integers and *mn* is even, prove that *m* or *n* is even." To prove this we assume that *mn* is even and *m* and *n* are odd. Then we may write $m = 2s + 1$ and $n = 2t + 1$ for some integers *s* and *t*. Then $mn = (2s + 1)(2t + 1) = 4st + 2s + 2t + 1 = 2(2st + s + t) + 1$, which is odd. Since this contradicts the assumption that *mn* is even, the proof is complete.

PROOF BY CASE ANALYSIS

A common way to construct a direct proof is to examine all possible cases. Consider the statement "If the product of two integers is odd, then both of them are odd." We begin by converting words to symbols by denoting the two integers by *m* and *n* and consider four cases

CASE 1. *m* and *n* are even. In this case we can write $m = 2s$ and $n = 2t$ for some *s* and *t*. Then $mn = 2s2t = 2(2st)$ and *mn* is even.

CASE 2. *m* and *n* are odd. In this case we can write $m = 2s + 1$ and $n = 2t + 1$ for some *s* and *t*. Then $mn = (2s + 1)(2t + 1) = 4st + 2s + 2t + 1 = 2(2st + t + s) + 1$ and *mn* is odd.

CASE 3. *m* is even and *n* is odd. In this case we can write $m = 2s$ and $n = 2t + 1$ for some *s* and *t*. Then $mn = 2s(2t + 1) = 4st + 2s = 2(2st + s)$ and *mn* is even.

CASE 4. *m* is odd and *n* is even. This case is the same as Case 3 since *m* and *n* are interchangeable.
To complete the proof we observe that the only case that does not yield a even product is when both *m* and *n* are odd.

PROOF BY EXPERIMENT

Although you cannot generally prove statements by experiment, many proofs can be done with the help of experimenting. One typically looks at simple cases to gain insight and this insight results in a proof.

Consider the statement "Every odd integer is the sum of two consecutive integers." Trying a few small cases we have
$3 = 1 + 2$
$5 = 2 + 3$
$7 = 3 + 4$.
It seems that a general pattern is $2n + 1 = n + (n+1)$ and indeed this gives us a proof.

Here is another example. Consider the statement "Prove that every positive odd integer is the difference of two squares." Since the statement of the problem tells us that we must look at differences of two squares, we begin by listing the small squares and taking some differences to see if we can detect a pattern. The first six squares are:
$0^2 = 0$
$1^2 = 1$
$2^2 = 4$
$3^2 = 9$
$4^2 = 16$
$5^2 = 25$.
Taking differences of successive squares we have:
$1^2 - 0^2 = 1$
$2^2 - 1^2 = 3$
$3^2 - 2^2 = 5$
$4^2 - 3^2 = 7$
$5^2 - 4^2 = 9$.
Although that it appears that by taking the difference of successive squares we will obtain every odd positive integer we still must prove that this is the case. Observing that $(n + 1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1$ is the entire proof. Moreover, this proof is valid for all odd integers, not just the positive odds.

IF AND ONLY IF PROOFS

When trying to prove an "if and only if" statement it is highly recommended not use an "if and only if" argument. They are tricky to get correct for beginners. Instead, if you are asked to prove that A is true if and only if B is true, first assume that A is true and use this assumption to prove B is true. Then begin all over by assuming that B is true and use that to prove A is true. This approach requires two independent proofs.

PROVING TWO SETS ARE EQUAL

Whenever you are asked to prove a set A is equal to a set B, proceed by assuming an element x belongs to A and use the defining property of A to show that x belongs to B. Then assume some element x belongs to B and use the defining property of B to prove that x belongs to A.

Here is an example. To prove that $\{(n+1)^2 - n^2 |$ where n is an integer$\}$ is the set of all odd integers we let $(n + 1)^2 - n^2$ be any member of the left side. Since $(n + 1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1$ we have shown that $(n + 1)^2 - n^2$ is a member of the right side. Now let k be any member of the right side. Since k is odd it can be written in the form $2n + 1$ for some integer n and since $2n + 1 = (n+1)^2 - n^2$ we have shown that k is a member of the left side.

DISPROVING

Although "proof by example" is not legitimate, you can disprove statements by way of a single example. Consider the statement "The sum of two irrational numbers is irrational." To disprove this statement we simply observe that $\sqrt{2}$ and $-\sqrt{2}$ are irrational but $\sqrt{2} + -\sqrt{2} = 0$ is rational.

PROVING UNIQUENESS

To prove an object is unique assume that a and b are two objects with the desired property and show this property together with other known information to show that $a = b$. To illustrate, consider the statement "For any real number r the equation $x^3 = r$ has a unique real number solution." To prove this statement assume that a and b are both solutions of $x^3 = r$ and use algebra and properties of real numbers to prove that $a = b$.

LOOK BACK

After you complete a proof, look back to see if you used all the hypotheses. Also, be sure that you have provided reasons for each step.

NEGATING STATEMENTS

Be careful with negations. The negation of "for all" is "there is at least one" and vice versa. For example, the negation of the statement "For every real number x, $x^2 > 0$ " is "There exist at least one real number x for which $x^2 \leq 0$." Conversely, the negation of "There exist at least one real number x for which $x^2 \leq 0$" is "For every real number x, $x^2 > 0$." These are easy to remember by thinking of a statement such as "Everyone passed the exam." The negation is "At least one person failed the exam." The negation of "At least one person failed the exam" is "Everyone passed the exam."

PROVING A FUNCTION IS ONTO

Proving a function is "onto" causes confusion among many students. If you wish to prove that some function f from A to B is onto, let b denote any element of B. You must find some x in A such that $f(x) = b$ (think of b as given and x as an unknown). To do this replace $f(x)$ by the actual formula for $f(x)$ and then solve for x in terms of b. You must check to see whether the solution you obtained is in set A. Here is an example. Say you are asked to prove that $f(x) = x^2$ from the positive reals to the positive reals is onto. We let b be any positive real. Then we must solve the equation $x^2 = b$ for x. Noting that $x = \sqrt{b}$ is a positive real solution proves that f is onto. In contrast, if we have the same function from the positive rationals to the positive rationals the function is not onto since there is no rational solution of the equation $x^2 = 2$.