More about Homework and Proofs with Examples

There are two main ways to write proofs: in mathematical shorthand or in complete sentences with limited symbols. How many mathematical symbols you should use in a proof depends on the situation. In our class, or if you ever submit a paper to a journal, you should use as few symbols as possible (for our class, limit yourself to the acceptable symbols listed in the syllabus) and write in complete, grammatically correct sentences. If you are proving something for yourself or are in a class where the instructor does not care how many symbols you use, you can use as many mathematical or shorthand symbols as you want. In either situation, your job, when writing a proof, is to clearly communicate your solution to a reader who does not know whether the statement is true or not. You are trying to convince a skeptical reader that the statement is true.

I will accept either handwritten or typed homework. If you handwrite your proofs, they **must be legible**. If you type your proofs (in latex or Word), the formatting must be correct; computer programs can have trouble with mathematical notation if you do not know what you are doing. If you scan your homework and email it to me, it must be in PDF format. Also, make sure you can read the scanned document before sending it. Be sure your name is on both the scanned document and in the name of the file. In all cases, if I cannot read what you submit, you cannot get a good grade.

If you write homework questions (or test questions) on your own paper and not on the provided sheets, you must write out the full question as given, including any directions. Write the question in ink so that it is distinctive from your solution. If you type the homework set, bold the question to distinguish it from your solution.

There will be chances to revise your homework. For revisions, you must turn in both the original homework question as well as the revised version. If you turn in a revised version, your final score for that homework set will be the average of your grades on the original and revised versions. If you do not turn in a revised version, your score from the original version will be what you get on that homework set. In most cases, grades on revised work should be better than on the original. However, that may not be true if you do not follow the recommended changes, if you do not include the correct parts from the original question, or if you do not make any changes. In these cases, your score could decrease.

Both the original homework set and the revised homework set must be turned in on time, which means by midnight the Thursday it is due. Homework sets will be due every Thursday – one week after they are distributed. See the class website for exact due dates. Revisions to homework sets are due on the Thursday of the week after the graded original homework set is returned. For example, if homework set 1 is handed back on January 22, then revisions to homework set 1 will be due January 29. Homework sets (or revisions) turned in late will not be accepted.

Stringing equations together is how mathematicians write, but the order of the equalities is very important. Here is an example of two ways to prove a statement. Both are correct proofs; however, only the second way will be receive full credit in our course.

Statement: Let a, b, c, and d be integers. If a divides c and b divides d, then ab divides cd.

Proof (way 1: using symbols):
Let $a, b, c, d \in \mathbb{Z}$ and assume $a|c$ and $b|d$.
$\Rightarrow\ \exists r, s \in \mathbb{Z}\ \ni\ c = ar$ and $d = bs$ by the definition of divides.
$\Rightarrow\ cd = (ar)(bs) = a\big(r(bs)\big) = a\big((rb)s\big) = a\big((br)s\big) = a\big(b(rs)\big) = (ab)(rs)$ by the associative and commutative properties of integers.
$\therefore\ ab|cd.$

Proof (way 2: using sentences not symbols):
Let a, b, c, and d be integers. Assume a divides c and b divides d. Then by the definition of divides, there exist integers r and s such that $c = ar$ and $d = bs$. Thus, $cd = (ar)(bs) = a(r(bs)) = a((rb)s) = a((br)s) = a(b(rs)) = (ab)(rs)$ by the associative and commutative properties of integers. Therefore, by the definition of divides, ab divides cd.

In the proof above, we know $cd = (ar)(bs)$ by substitution. We do not directly know that $cd = (ab)(rs)$, but we do know by successive applications of the associative property of multiplication that $(ar)(bs) = a(r(bs)) = a((rb)s)$. Also, multiplication of integers is commutative so $rb = br$. Using both properties, we obtain the following string of equations:

$$cd = (ar)(bs) = a(r(bs)) = a((rb)s) = a((br)s) = a(b(rs)) = (ab)(rs)$$

What you care about in this proof is showing that cd is an integer multiple of ab. So start the string of equations with $cd =$. Any of the following three products could be on the right hand side of the equals: $(ar)(bs)$, $c(bs)$, or $(ar)d$. The first is the best choice since we eventually want to get $(ab)(some\ integer)$. Include the entire string to show how this is accomplished.

Basic Scheme for writing a proof of an IF…, THEN… statement

Here is another fairly simple statement to prove about integers. We will go through the steps of the proof one sentence at a time. The GCD Theorem, Divisor Theorem, and the GCD=1 Theorem were on a sheet handed out on the first day of class and can be found on the class website.

Statement(P): Let a, b, d, r, and s be integers. If $a = dr$, $b = ds$, and $d = \gcd(a, b)$, then $\gcd(r, s) = 1$.

Step 1: If any terms are defined, be sure to include them at the beginning of your proof.
Step 1 for (P): Let a, b, c, and d be integers.
Step 2: Change the word IF to ASSUME and continue with the exact statement that follows the IF until you reach the comma directly before the THEN. Change the comma to a period, and STOP. This is the entire next sentence of your proof. **Do not write anything else in this sentence.**
Step 2 for (P): Assume $a = dr$, $b = ds$, and $d = \gcd(a, b)$.
Step 3: For the next sentence(s), write down whatever useful equations or other conclusions you can based on either definitions of the terms used in the first sentences or from previously proved theorems or exercises. For theorems and exercises, **you must identify which one(s) you are using**. Also, remember to define what each new letter represents. For the first few weeks, every letter will represent an integer. Later, they will also represent other objects.
Step 3 for (P): Then by the GCD Theorem, $d > 0$, and there are integers f and g such that $d = af + bg$.
Step 4: Once you have applied the definitions/theorems/exercises to get some new equations or other information, do something with them. So, what do you do? Try stuff on a scratch piece of paper until you find something useful, but in the proof that you submit, only mention the stuff that actually worked. At this point, it is often useful to try to work backwards from what the conclusion is supposed to be. Are there any theorems/definitions/exercises whose result is the conclusion for which you are looking? *The most important thing to remember is this is an Algebra class so **substitution** is your friend.* In this particular problem, we are asked to prove that the greatest common divisor of r and s is 1. So, if you cannot think of anything else at this point, give $\gcd(r, s)$ a name, without saying that it is 1. You are not allowed to say it is 1 until you have proved that it is so.
Step 4 for (P): Let $e = \gcd(r, s)$. Then by the GCD Theorem, $e > 0$, and there are integers k and m such that $r = ek$ and $s = em$.
Step 5: Repeat Step 3 using these new equations. Again try substitution and manipulation until you find something useful, perhaps based on previous theorems or proofs.

Step 5 for (P): Since both d and e are positive integers, $1 \leq e$ and $d \leq de$. By substitution, $a = dr = dek$ and $b = ds = dem$. Thus, de divides both a and b. Hence, de divides d by the GCD Theorem. Since both d and e are positive integers, $de = d$ by the Divisor Theorem. Another application of the Divisor Theorem yields $1 = e$. Therefore, $\gcd(r, s) = e = 1$.

The following is a very complete (far too complete) proof of the statement above. It differs from the previous one by using the equation $d = af + bg$ but not using $e = \gcd(r, s)$.

Proof (way 3: too verbose): Let a, b, c, and d be integers. Assume $a = dr$, $b = ds$, and $d = \gcd(a, b)$. Then by the GCD Theorem, $d > 0$, and there are integers f and g such that $d = af + bg$. Thus, by substituting dr for a and ds for b, we have $d = (dr)f + (ds)g$. By the associative property of multiplication, $(dr)f = d(rf)$ and $(ds)g = d(sg)$. So, by substituting $d(rf)$ for $(dr)f$ and $d(sg)$ for $(ds)g$, we have $d = d(rf) + d(sg)$. By subtracting d from both sides and substituting $d \cdot 1$ for d, we have $0 = d(rf) + d(sg) - d \cdot 1$. By factoring out d using the distributive property, we get $0 = d[rf + sg - 1]$. Since $d = \gcd(a, b)$, it is a positive integer by the GCD Theorem. Also, $rf, sg, rf + sg$, and $rf + sg - 1$ are integers since the product, sum, and difference of two integers is an integer. Thus, we must have $0 = rf + sg - 1$ since a product of two integers being 0 implies at least one of them is 0, and we know that d is a positive integer, so it is not equal to 0. By adding 1 to both sides, we obtain $1 = rf + sg$. Since $r = r \cdot 1$ and $s = s \cdot 1$, 1 divides both r and s. We also know that 1 is a positive integer. Therefore, using the fact that statement (3) of the GCD Theorem implies statement (5) of the GCD Theorem, we have that $\gcd(r, s) = 1$.

While this proof is correct and at least for the beginning of the semester would receive full credit, it is far too verbose. No one wants to read a proof like this one. A better version is as follows:

Proof: Let a, b, c, and d be integers. Assume $a = dr$, $b = ds$, and $d = \gcd(a, b)$. Then by the GCD Theorem, $d > 0$, and there are integers f and g such that $d = af + bg$. Thus, $d \cdot 1 = d = af + bg = drf + dsg = d[rf + sg]$. Hence, $1 = rf + sg$ by the Divisor Theorem. Therefore, $\gcd(r, s) = 1$ by the GCD=1 Theorem.

Writing up a Proof – an Outline

Your basic approach to actually writing a proof (once you figure out what steps to use) should be to try to write so that someone else in the class would be able to easily follow, understand, and believe the steps. Your proof must include *justification* (generally what theorems allow you to make a particular statement or conclusion), and should include enough *detail* so that no one has to guess what it is that your proof is trying to prove. The best way to accomplish this is to simply make the first sentence(s) tell the reader what you are assuming to be true; then end with "Therefore, (whatever the conclusion is supposed to be)." When in doubt, put in more steps rather than fewer. If your proof is correct, I will not count off if you have written more than is necessary as long as the extra information is related and not wrong. Also, if the proof involves showing one thing is equal to another, it is always wrong (and sometimes dangerous) to put in an equation before you actually have it established. We are not solving equations. We are *proving* things. **Start with one side, and work your way through until you have what you were asked to prove.** It is a good idea to outline the proof on a scratch piece of paper (many people use symbol notation here). You can take a little bit more liberty here, but keep in mind that you want to start with what is on one side and transform it into the other side. There is no need to include your scratch work in what you submit for a grade. After you have the outline of the proof from your scratch work, write up the proof in the proper format. Just like if this were an English class where your professor would not accept a handwritten draft for the final version of an essay, your proofs should look like polished essays that happen to include mathematical terms and symbols.

Checklist for Grading Proofs/Homework Sets

Logic/Math (50%):

- Are all assumptions stated?
- Are all steps included?
  - Is each step proved?
- Does each step follow in a logical way?
- Have all theorems, lemmas, corollaries, and definitions been cited?
  - Have all theorems, lemmas, corollaries, and definitions used been proved in class or were covered in a section of the textbook already covered?
- Has the conclusion been stated?

Format (50%):

- Is the writing legible?
- Is everything written in complete sentences?
- Are all words spelled correctly?
- Was the correction punctuation used, including periods at the end of the sentences?
- There is not an over use of symbols.
  - For example, the proof used "x is in A" as opposed to $x \in A$.
  - No abbreviations were used.
  - Did not use any of the "forbidden symbols": $a|b, \div, \forall, \exists, \Longrightarrow, \Longleftrightarrow, \Longleftarrow, \therefore, \because, \ni, , a/b, \frac{a}{b}, \&$

Extra Formatting for Revisions:

- Were the revisions written on a separate piece of paper?
- Was the entire question and work that was revised written out?
- Was the original, graded homework set attached to the revision?