LECTURE 9 EXCERCISE SOLUTIONS

In several instances, when writing up these solutions, I have gone to some lengths to directly phrase things in terms of definitions you know, or logical statements you should be considering. This is just to emphasize as best I can how all of the work fits together into a coherent whole. I won't necessarily hold you to the same rigidity I present here, though I would like a decent level of coherency.

While I am breaking the norm and speaking to you up here, let me mention as well (since it is driving me nuts), that proof by example is rarely appropriate. Consider the following proof by example: *All odd numbers greater than 1 are prime. 3 is prime, 5 is prime, 7 is prime, and the pattern continues. Therefore all odd numbers greater than 1 are prime.* Let's just ignore 9, for the moment. My point is, if you are proving a universal, by and large, proof by example does not work.

Problem. 1: Prove the following is *false*: $\forall n$ ($n^2 + n + 41$ *is a prime number*).

Solution. To prove the above statement false is to prove the opposite is true, that $\exists n$ ($n^2 + n + 41$ *is not a prime number*). And the easiest way to prove an existence statement (often) is to find an example. Recall that a prime number is one that is not divisible by any number but itself and 1. Consider, in this case, $n = 41$, or $41^2 + 41 + 41$. Without even having to compute too much, we have that $41^2 + 41 + 41 = 41(41 + 2) = 41 * 43$. That is clearly not prime. Therefore, there exist n such that $n^2 + n + 41$ is not prime. $n = 41$ is such a number, though there are many more. In any case, $\forall n$ (n^2+n+41 *is a prime number*) is false.

You may well ask, *Yes, but why did you pick n = 41?* I knew that I needed $n^2 + n + 41$ to be divisible by a number. The easiest way for a sum to be divisible by a number is if each term is divisible by a number. Since the first two terms are clearly divisible by n, and the last term is only divisible by 1 or 41, that immediately suggested $n = 1$ or $n = 41$. $n = 1$ gives 43, which is prime, but $n = 41$ works.

Common Problems. Note that this is essentially proving a statement of existence, and that is pretty much the -only- case where proof by example is okay.

Everyone was mostly okay on this problem. Some people chose some very strange values of n, I must say. Where I took off generally fell in the following: You didn't offer some conclusion, such as *For this value of n,* $n^2 + n + 41$ *is not prime, therefore the statement is false.* You offered up an example and claimed that it wasn't prime, but you didn't -show- it wasn't prime. Primality is non-trivial. Would you believe me if I said $2^{109} - 1$ wasn't prime? The factors are very non-trivial. What about $2^{107} - 1$? It is important to justify

yourself. Anyway. The last things I knocked off points for were making erroneous logical statements (things that didn't follow), other unjustified claims, or simply saying things I didn't understand.

Problem. 2: Prove that, if a divides b, then a^n divides b^n for all n.

Solution. Because a divides b, we know that there exists some number k such that $b = k*a$.

Then for any n, $b^n = (k*a)^n = k^n * a^n$. Therefore, there exists a number k' (namely $k' = k^n$), such that $b^n = k' * a^n$. Therefore, a^n divides b^n.

Common Problems. Various errors for this problem. If you introduced the variable k without saying what it was, or why it existed (citing the definition of divides, for instance), then you lost a point. Some people would introduce a k everytime something divided soething else, without specifying that it would be a *different* k. Also, many notational errors here. $adividesb$ is represented as $a|b$. It is a proposition. b/a is a value. Also, when you finish a problem, always conclude.

One thing I saw a lot of was people considering b/a or b^n/a^n. Note that for integers a, b, both these exist - though they may be fractions, not natural numbers. To be relevant to the problem, you need to be specific that they happen to be integers, since a divides b.

Mostly people lost points if I couldn't tell what you were doing, or were doing something that didn't seem to lead to the necessary conclusion.

Problem. 3: Prove that 2 divides $k * (k + 1)$ for all k.

Solution. We can consider two cases. Any natural number is odd (of the form $2n + 1$ for some n) or even (of the form $2n$ for some n).

Case 1: *Consider k even.* Then, for some natural number n, $k = 2 * n$. In that case, $k * (k + 1) = 2 * n * (2 * n + 1)$. Thus we have, for some natural number q (namely $q = n * (2 * n + 1)$), that $k * (k + 1) = 2 * q$. Hence, 2 divides $k * (k + 1)$.

Case 2: *Consider k odd.* Then, for some natural number n, $k = 2 * n + 1$. In that case, $k*(k+1) = (2*n+1)*(2*n+1+1) = (2*n+1)*(2*n+2) = (2*n+1)*(n+1)*2$. Thus we have, for some natural number q (namely $q = (2*n+1)*(n+1)$), that $k*(k+1) = 2*q$. Hence, 2 divides $k * (k + 1)$.

Since any natural number k must satisfy one of these two cases, for any natural number k we have that 2 divides $k * (k + 1)$.

Common Problems. One thing I'm seeing that really bothers me is people using 2 *divides* $k * (k + 1)$ as a hypothesis. It is not. It is what we are trying to prove true. You cannot assume it to be true starting out. If you start out with the equation $k * (k + 1) = 2 * z$ for natural number z, and then operate on that, you are assuming what you want to prove, in that you are assuming z exists. Bad!

Again, in general, be sure to quantify your variables. If you introduce a new variable, or some value that must exist, say why it must exist. One other thing a lot of people are doing is phrasing this in terms of *even* and *odd* rules. And that's mostly fine, if you're clear enough in what you're saying.

Aside: But there is an advantage to doing it out as I've done here, or even more simply, in that the argument is more tight and well defined. Using words can often hide or gloss over details that need to be attended, while writing it out in math, if you will, everything is right there and you can see how it fits together. I know I have been adamant that words are good in a proof, and they are. But words should be used to explain what you're doing, not to do it.

Lastly, just to round out my usual litany of complaints, this is yet another example of a problem that cannot be proven by example.

Problem. 4: Prove that if 2 divides $m - 1$, 8 divides $m^2 - 1$.

Solution. The first thing I always want to do when I see a difference of squares is to factor it.

$$m^2 - 1 = (m - 1) * (m + 1)$$

This immediately looks promising, since it contains an '$m - 1$' expression, and we have information about that.

If 2 divides $m - 1$, then for some number k, we have that $m - 1 = 2 * k$. Note too, $m + 1 = m - 1 + 2 = 2 * k + 2 = 2 * (k + 1)$.

Substituting $m - 1 = 2 * k$ and $m + 1 = 2 * (k + 1)$ into the expression, we get that $m^2 - 1 = (2 * k) * (2 * (k + 1))$, or

$$m^2 - 1 = 4 * k * (k + 1)$$

Note from problem 3 that, for any k, $k * (k + 1)$ is divisible by 2. Let $k * (k + 1) = 2 * q$ for some number q. Substituing that into our expression, we get

$$m^2 - 1 = 4 * (2 * q)$$

Or

$$m^2 - 1 = 8 * q$$

What we have shown is that, if 2 divides $m-1$, $m^2-1 = 8*q$ for some number q. Therefore, if 2 divides $m-1$, 8 divides m^2-1.

Common Problems. One common thing I'm seeing goes something like this, *Since* $m-1$ *is even,* m *is odd, thus* m^2 *is odd, and* m^2-1 *is even. Since 2 divides* m^2-1 *and* $8 = 2^3$*, 8 divides* m^2-1. This does not follow. For instance, 6 is even, but 8 does not divide 6. Similar but slightly bettr, I'm seeing a lot of, *if* $m-1$ *is even,* $m+1$ *is divisible by 4.* It is true that one of them has to be divisible by 4, but why $m+1$? Not to mention the fact that you need to -prove- that one of them is divisible by 4 (which is basically what we accomplish in our appeal to problem 3 - it's buried in there). Most mistakes stemmed from people declaring numbers to be of a particular form that they didn't have to be.

Suppose you were going along like the first hypothetical proof and you wanted to test yourself. You might choose some odd m and plug in, to see if 8 divided m^2-1. However, (since we're trying to prove it), this will -always- be true. But if you read the proof, the logic isn't that an odd squared minus one is divisible by 8. The proof says that an odd minus one is divisible by 8. The fact that we are considering a square vanishes from consideration when we declare m^2 to be odd and leave it at that. So the true test is to pick an odd number, M and see if $M-1$ is divisible by 8. Taking $M = 11$ shows the flaw in that argument.