Week 2 tutorial solutions

General hints/notes

Emphasis should be writing proofs in good style. Stuff to check:

- Proof must be IN LOGICAL ORDER.
- Use a separate piece of scratch paper. Work backwards from conclusion on scratch paper, then rewrite in logical order for final proof.
- Connector words, punctuation make it easy to read. Use words (e.g. "therefore") rather than funny little patterns of dots and arrows.
- Alternate outlines (e.g. contrapositive): proof should start by informing the reader of the new outline. State contrapositive explicitly.
- Counter-examples should be concrete (e.g. specific numbers)
- At the start of proof, introduce variables and "suppose" assumptions
- Middle of proof: use textbook definitions of concepts (e.g. rational)
- Inequalities: do the algebra, don't reason from (alleged) maximum/minimum values
- Justifications: only on interesting steps. Algebra steps don't need comments.
- Proof should end at the conclusion (not e.g. one step before)

1.2

(b) This universal claim is false, as demonstrated by the following counterexample. Suppose that $p = 1$ and $q = 2$. Then $(p + q)^2 = 9$, but $p^2 + q^2 = 5$, so $(p + q)^2 \neq p^2 + q^2$.

Commentary: There are many possible answers; you do not need to pick the "smallest" counterexample but you should pick one that is easy to follow - e.g. $p = 13, q = 54$ *is technically correct but a bad choice. It is also technically possible to classify* all *possible counterexamples (e.g.*

something like "The claim is false, as shown by any p and q that are both non-zero."), but you should **not** *attempt to do so in your solution since providing a single counterexample is sufficient and much easier.*

(c) The claim is not true. Suppose that w, x, y, z are $0, 1, -1000, -5$, respectively. These satisfy the conditions that $w < x$ and $y < z$. However, $wy = 0 > -5 = xz$, so $wy \not< xz$.

Commentary: Again there are many answers, but they may be harder to find than in part (b). I found this answer by checking what happens if $w = 0$. Checking "edge cases" like that is often a good place to start because you may find that things simplify/cancel - in this case, it becomes a search for x, y, z where $0 < x$, $y < z$, $0y = 0 \geq xz$, and suddenly I have lots of freedom to choose y since it disappeared from the final inequality, and I also have clear direction of how to continue since I see x must be positive while xz should be negative (or zero).

1.3d

We will proceed by proving the contrapositive, i.e. we will show that for every real number x, if $x < 2$ and $x \geq 1$ then $x^2 - 3x + 2 \leq 0$. So let x be a real number and suppose that $x < 2$ and $x \geq 1$. Since $x < 2$, $x - 2 < 0$. Since $x \geq 1$, $x - 1 \geq 0$. Therefore $(x - 1)(x - 2) \leq 0$. So $x^2 - 3x + 2 = (x - 1)(x - 2) \leq 0$, which is what we needed to prove.

1.4a

Let k be an integer and suppose that $k > 4$. This gives us $k^2 > 4k$, and also $2k > 8$ so $2k > 1$. Thus we have $k^2 > 2k + 2k > 2k + 1$, so $2k + 1 < k^2$, QED.

Commentary: A proof with inequalities will often include a step that seems to come out of nowhere - e.g. here, it is clearly true that when $2k > 8$ we also have $2k > 1$, but how did we know to make that particular leap instead of many other true statements we could have said (like $2k > 0$, or $2k > -100$)? The key is that on your scratch paper beforehand, you should be trying to make the inequalities look as similar to each other as possible - e.g. in this case one of them has a k^2 so I tried out squaring the other one (which didn't *lead anywhere useful, oh well) and also multiplying it by k, and once I had both $k^2 > 4k$ and $k^2 > 2k + 1$ written on the scratch paper, it became clear that $4k > 2k + 1$, i.e. $2k > 1$, would be a useful fact to derive which would allow me to link them.*

2.2

Common misconception: *You cannot solve parts a and b by setting up a system of two equations with just two variables, e.g. in part b it is not accurate to say "$x = 6a + 5$ and also $x = 10a + 3$". It is technically accurate (but confusing) to say "$\exists a, x = 6a + 5$, and also $\exists a, x = 10a + 3$" because the quantifiers make clear the separate scopes, but best to just use separate variable names (i.e. it is correct to say "there are a and b for which $x = 6a+5$ and $x = 10b + 3$").*

(a) There is no such x. From the first congruence, we would need $x = 7+9p = 1+3(2+3p)$ for some integer p, so $remainder(x, 3) = 1$. From the second congruence, we would need $x = 5 + 12q = 2 + 3(1 + 4q)$ for some integer q, so $remainder(x, 3) = 2$. There is no number which has two different remainders when divided by 3.

Commentary: How did we know to take remainders at all? They're frequently useful once you're already in the world of modular arithmetic, so worth a try. How did we know to take remainders dividing by 3 specifically? Notice that if all you have is the congruence $x \equiv 5 \pmod{12}$, then you actually can't determine the value for many remainders, like $remainder(x, 7)$. (Try it!) Given congruences mod 9 and 12, $remainder(x, 3)$ is the only remainder that can be calculated from both of them.

Alternate solution: There is no such x. From the first congruence, we would need $x = 7 + 9p$ for some integer p, and from the second congruence, we would need $x = 5 + 12q$ for some integer q, so $7 + 9p = 5 + 12q$. This rearranges to $3p - 4q = \frac{2}{3}$. But then there are no possible values for p and q, since the left hand side will always be an integer while the right is not.

Don't worry about how exactly to formalize this proof - it's actually best presented as a "proof by contradiction", but we haven't covered that style of proof yet.

(b) Yes, for example $x = 23$. $23 = 6 \cdot 3 + 5$, and also $23 = 10 \cdot 2 + 3$.

2.3a

The claim is false. For a counterexample, consider $p = r = 3$ and $q = 2$. Then $\gcd(p, q) = \gcd(q, r) = 1$, but $\gcd(p, r) = 3$.

Commentary: "$\gcd(p, q) = 1$" can be thought of as "p and q have no common factors"; I found that formulation helpful for developing this counterexample.

2.4a

Let a, b, c be integers and suppose that $a|b$ and $b|c$. Then by the definition of divides, $b = an$ and $c = bm$, for some integers n, m. Then $c = (an)m = a(nm)$. nm is an integer because n and m are integers, so $a|c$ by the definition of divides.