Some Solutions for Week 1 Homework

7a). Suppose $b|a$, so by definition $a = bq$ for some integer $q$. Then $ac = (bq)c = b(qc)$, since multiplication is associative. Thus, $b|ac$.

Editorial comment: As this proof makes clear, there is nothing more to this than the definition of divisor and associativity of multiplication. Any “proof” that doesn’t make this clear is probably not very good.

One can prove parts b and c along similar lines, just using the definition of divisor and the axioms for addition and/or multiplication.

9a). Suppose $b|a$ and $b|(a + c)$. Then by #7c, $b|ma + n(a + c)$ for all $m, n \in \mathbb{Z}$. In particular, $b$ divides $-1 \times a + 1 \times (a + c) = (-a + a) + c = c$.

Editorial comment: Notice how I snuck in several axioms and previous results here. In great, gory detail, I’d write $-1 \times a$ is the additive inverse of $a$ by a previous result. By definition of 1 as the multiplicative identity, $1 \times (a + c) = a + c$. By associativity, $-a + (a + c) = (-a + a) + c$. By definition of additive inverse, $-a + a = 0$. Finally, by the definition of additive identity, $0 + c = c$.

Deciding how much you can get away with (sneaking stuff in like this) is perhaps the most difficult part of writing proofs. You have to take into account your audience, what’s lead up to your proof, and other factors. For the purposes of this class, it’s probably best to err on the side of too much detail rather than too little. When you’re really in doubt, come see me about it. I’m there to help.

9b). Suppose $b|a$. If $b|(a + c)$, then $b|c$ by 9a). Thus, if $b \nmid c$ then if $b \nmid (a + c)$.

17. Suppose $a$ and $b$ are non-zero integers. Let $d$ be the greatest common divisor of $a$ and $b$ and let $d'$ be the “largest” common divisor, i.e., the greatest common divisor via the new definition.

Since $d$ is a common divisor of $a$ and $b$, we have $d \leq d'$ (this is using the definition of $d'$ as the “largest” common divisor). Since $d'$ is a common divisor of $a$ and $b$, we have $d'|d$ (this is using definition 1.1.5). Since $d$ is positive (also part of definition 1.1.5, you’ll note), this implies that $d' \leq d$. Thus $d' = d$.

Editorial comment: The phrase “this implies” above is really hiding more detail. Why is it that for positive integers $a$ and $b$, $a|b$ implies that $a \leq b$? You could definitely argue that this is
something requiring proof at this point. If that’s the way you feel (and even if it isn’t!), you should try to prove this.