

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 need 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 $b \nmid (a + c)$. (In fact, this and the first part are logically equivalent.)

17. First suppose $r_1 = r_2$. Then

$$\begin{aligned} a - b &= nq_1 + r_1 - (nq_2 - r_2) \\ &= nq_1 - nq_2 + r_1 - r_2 \\ &= n(q_1 - q_2), \end{aligned}$$

so $n|(a - b)$. (This was the easy part.)

Next suppose $n|(a - b)$. Similar to what we did above, we have $a - b = n(q_1 - q_2) + (r_1 - r_2)$. Clearly $n|n(q_1 - q_2)$, so by 9a) we have $n|(r_1 - r_2)$. Now we use the hypotheses $0 \leq r_1, r_2 < n$ to

see that $-n < r_1 - r_2 < n$. In other words, $|r_1 - r_2| < n$. But n divides $r_1 - r_2$, so we can write $r_1 - r_2 = nz$ and

$$n \cdot 1 = n > |r_1 - r_2| = n \cdot |z|.$$

Recall that 1 is the smallest positive integer (a seemingly silly, yet surprisingly important result).

Thus, $|z| = 0$, $z = 0$ and $r_1 - r_2 = 0$, so that $r_1 = r_2$.

Editorial comment: Your proof absolutely must use the hypotheses on r_1 and r_2 , since otherwise it's wrong. For example, we certainly have $5 = 2 \cdot 1 + 3$ and $7 = 2 \cdot 3 + 1$. Here $2|(5 - 7)$ but $3 \neq 1$.

Finally, please be sure your proofs use grammatically correct sentences (including punctuation). The mathematical symbols should be parts of the sentence (nouns, verbs, etc.) and you should be able to read it aloud and have it make sense. Also, as a matter of style, one should never start a sentence with a mathematical symbol.