Math 302 Spring 2017 Homework #1 - Solutions

Ch. 1.1 #7: Prove that the square of any integer a is either of the form $3k$ or of the form $3k + 1$ for some integer k. Use the Hint (always use the hints – that's what they're there for!). Since a is an integer it can be written as $3q$, $3q + 1$ or $3q + 2$ where q is an integer (by the Division Algorithm). We now check each of these cases: $(3q)^2 = 9q^2 = 3(3q^2)$. By setting $k = 3q^2$, we see that we have the form $3k$. $(3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2) + 1 = 3k + 1$, now with $k = 3q + 2$. Lastly, $(3q + 2)^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 = 3(3q^2 + 4q + 1) + 1 = 3k + 1$ (where $k = 3q^2 + 4q + 1$). By the way, to be really complete, we should mention that in all cases, the number we call k is indeed an integer because the integers are closed under addition and multiplication.

Ch. 1.1 #10: Let n be a positive integer. Prove that a and c leave the same remainder when divided by n if and only if

$$a - c = nk \text{ for some integer } k.$$

A note on notation: Some of you used some very incorrect notation in stating this theorem. Instead of writing " when a is divided by n and c is divided by n", you wrote "$\frac{a}{n}$ and $\frac{c}{n}$". This is completely incorrect. $\frac{a}{n}$ and $\frac{c}{n}$ are simply numbers, they do not represent any kind of sentence or statement. Do *not* use this notation to describe division. It can only be used (and in this class, rarely) to indicate the arithmetic result of division.

$\Rightarrow$: Suppose that a and c leave the same remainder (call it r) when divided by n. Then using the Division Algorithm, we can write

$$a = nq + r \text{ for some } q \text{ and } c = np + r \text{ for some } p.$$

But then

$$a - c = (nq + r) - (np + r) = n(q - p).$$

Setting $q - p = k$, we see that

$$a - c = nk.$$

(k is an integer because both q and p are integers, and the integers are closed under subtraction).

Note A: You do need to confirm that k is an integer; it's an important step in the proof!

$\Leftarrow$: Method 1: Now suppose that $a - c = nk$ for some integer k. Again we use the Division Algorithm to say

$$a = nq + r, \text{ while } c = np + s.$$

Notice that this time, I use different letters for both the quotients and the remainders, because I don't know that any of them are equal. But now

$$nk = a - c = (nq + r) - (np + s) = n(q - p) + (r - s).$$

Note B; At this point some of you, citing your work in proving the other direction, set $p - q = k$. But the variable k is also in use, and you have no reason to assume that the difference in the quotients $(p - q)$ is the same as the difference of the two numbers $(a - c)$. So those two numbers (k and $p - q$) may not be the same; in fact, it requires a proof (which follows) that it must be 0.

$$\text{So } (r - s) = nk - n(q - p) = n(k - q + p) = nt.$$

In other words, we see that $r - s$ is a multiple of n, that is $r - s = nt$ for some integer t. But $0 \le r < n$, and $0 \le s < n$, so we must conclude that $-n < r - s < n$, that is, $-n < nt < n$

(To see this, multiply $0 \le s < n$ by -1 to get $-n < s \le 0$, and add this inequality to $0 \le r < n$).

So now, if $-n < nt < n$, then $-1 < t < 1$, and the only integer between -1 and 1 is 0. So $t = 0$, so

$nt = 0$, that is, the only multiple of n that lies between $-n$ and n is 0, so $r - s = 0$, that is, $r = s$.
Note C: Here, you said that the only integer between $-n$ and n is 0, which is very incorrect (unless $n = 1$). The only *multiple* of n between $-n$ and n is 0, which is proved above.
Note D: This argument is of critical importance, and so if you omitted the argument that allows you to conclude that $r - s = 0$, you left out an important portion of the solution. So a and c leave the same remainder when divided by n.
Note E: You should state the argument that allows you to conclude that the only multiple of n strictly between $-n$ and n is 0: if $-n < nt < n$, then $-1 < t < 1$. Since the only integer strictly between -1 and 1 is o, $t = o$ and $nt = 0$.
Method 2: Again, suppose that $a - c = nk$ for some integer k, and as in Method 1, we use the Division Algorithm to write $a = nq + r$, while $c = np + s$. But now rewrite the equation $a - c = nk$ as $a = nk + c = nk + np + s = n(k + p) + s$. Now $0 \le s < n$, so it fits the criterion for the(unique) remainder in the Division Algorithm. So we must have $r = s$ and as an added bonus, $k + p = q$ (since both quotient and remainder are unique).

Ch. 1.1 #11: Prove: Let a and b be integers with $b \neq 0$. Then there exist unique integers q and r such that

$$a = bq + r \qquad \text{and} \qquad 0 \le r < |b|.$$

In plain English, we are now proving the Division Algorithm but extending it to negative divisors, so that finally we have a statement of the Division Algorithm where the dividend a can be any integer and the divisor can be any (nonzero) integer.
Case 1: $b \ge 0$. In this case, $|b| = b$, and we use the Division Algorighm: There exist unique integers q and r such that

$$a = bq + r \qquad \text{and} \qquad 0 \le r < b.$$

But since $b = |b|$, we get the statement we want.
Note F: We did not need to reprove the Euclidean Algorithm to establish the case for $b > 0$. The only thing that needs to be done is show that the remainder must satisfy the inequality, and since $b = |b|$, we can write $0 \le r < |b|$, but this step is required.
Note G: You don't need to completely re-do the full proof of the Division Algorithm. As we did with the first extension of the theorem (from $a \ge 0$ to all integers a), we use the first result (for $a \ge 0$) to prove the extension (if $a < 0$, then $-a > 0$). See Case 2 below.
Case 2: $b < 0$. Now let note that $-b > 0$, and $-b = |b|$. Using the Division Algorithm again, we see that there exist unique integers q_1 and r_1 such that

$$a\ (-b)q_1 + r_1 \qquad \text{and} \qquad 0 \le r_1 < -b, \text{ that is, } 0 \le r_1 < |b|$$

But now,

$$a = b(-q_1) + r_1 \qquad \text{and} \qquad 0 \le r_1 < |b|.$$

We're almost there: setting $q = -q_1$ and $r = r_1$, we get

$$a = bq + r \qquad \text{and} \qquad 0 \le r < |b|,$$

as desired.
Uniqueness follows easily: for $b > 0$, it was established as part of the Division Algorithm. If $b < 0$, suppose

$$a = bq_2 + r_2 \qquad \text{and} \qquad 0 \le r_2 < |b|.$$

We want to show that $q_2 = q$.

Then

$$a = (-b)(-q_2) + r_2 \qquad \text{and} \qquad 0 \le r_2 < |b|.$$

Since $-b > 0$, by the uniqueness part of the Division algorithm $-q_2 = q_1 = -q$, so $q_2 = q$, which is what we needed to prove. Also $r_2 = r$.

Note H: Uniqueness does have to be proved in the case where $b < 0$. As with the main result, we can refer back to the positive case.

Note I: You are having trouble with the absolute value. You wrote $|-b| = b$. This is not correct. The definition of $|b|$ is $|b| = b$ when $b \ge 0$ and $|b| = -b$ when $b \le 0$.

Ch. 1.2 #3: Prove If $a \mid b$ and $b \mid c$, then $a \mid c$. Since $a \mid b$,we can write $b = ax$, and since $b \mid c$, we can write $c = by$. But then $c = by = (ax)y = a(xy)$. Since xy is an integer, we can conclude $a \mid c$.

Ch. 1.2 #6: Prove if $a \mid b$ and $c \mid d$ then $ac \mid bd$. Since $a \mid b$, we can write $b = ax$ for some integer x, and since $c \mid d$, we can write $d = cy$ for some integer y. Than $bd = (ax)(cy) = (ac)(xy)$. Since xy will be an integer, we can conclude that $ac \mid n$. **Note G**: If you used Dr. Solheid's two-column format for an existential proof, that is perfectly OK. In most mathematical writing, that formality is dropped, and the information in Solheid's format is presented in more abbreviated form as shown above.

Note J: Be careful if you write fractions! You have to then keep track of which fractions represent integers.

Note K: You do need to show that xy is an integer.

Question A: If r is a solution to $x^2 + ax + b = 0$, then $r^2 + ar + b = 0$, so $-b = r^2 + ar = r(r + a)$ and $b = -(r^2 + ar) = r[-(r + a)]$. Since $r \ne 0$, we can say $r \mid b$. A number of you may have written the following: since r is a solution of $x^2 + ax + b = 0$, we can write $x^2 + ax + b = (x \pm r)(x - s)$, so $b = \pm rs$, and $r \mid b$. There are two problems with this proof. One is aesthetic: you are using facts beyond those established (or assumed) in this chapter. The other problem is more serious: how do you know that s is an integer? Establishing that requires extra fancy footwork.