Chapter 2 Solutions to Selected Exercises

Notes:

- The questions are in a separate PDF on LongFormMath.com.
- For most problems there are many correct solutions, so the below are not the only correct ways to solve the problems.
- If you spot an error, please email it to me at LongFormMath@gmail.com. Thanks!

Solution to Question 1. Let m and n be two odd integers. By Definition 2.2, this means that $m = 2a+1$ and $n = 2b+1$ for some integers a and b. Then,

$$mn = (2a+1)(2b+1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1.$$

And since, by Fact 2.1, $2ab+a+b$ is an integer too, we have shown that $mn = 2k+1$, where $k = 2ab+a+b$ is an integer. Therefore, by the definition of oddness, this means that mn is odd. □

Solution to Question 2. Assume that n is an odd number. By Definition 2.2, this means that $n = 2a+1$ for some integer a. Then,

$$\begin{aligned} n^2 + 6n + 5 &= (2a+1)^2 + 6(2a+1) + 5 \\ &= 4a^2 + 4a + 1 + 12a + 6 + 5 \\ &= 4a^2 + 16a + 12 \\ &= 2(2a^2 + 8a + 6). \end{aligned}$$

And since, by Fact 2.1, $2a^2 + 8a + 6$ is an integer too, we have shown that $n^2 + 6n + 5 = 2k$, where $k = 2a^2 + 8a + 6$ is an integer. Therefore, by the definition of evenness, this means that $n^2 + 6n + 5$ is even. □

Solution to Question 3. As an example, I chose $n = 3$. Then,

$$5n^2 + n + 3 = 5 \cdot 9 + 3 + 3 = 51,$$

which is odd. Now for the proof.

We will prove this by cases. Since n is an integer, by Fact 2.1 n is either even or odd.

<u>Case 1: n is even.</u> If n is even, then by the definition of an even integer, $n = 2a$ for some integer a. Then,

$$5n^2 + n + 3 = 5(2a)^2 + (2a) + 3 = 20a^2 + 2a + 2 + 1 = 2(10a^2 + a + 1) + 1.$$

Since a is an integer, also $10a^2+a+1$ is an integer, by Fact 2.1. Thus, we have shown that $5n^2+n+3 = 2k+1$ where $k = 10a^2 + a + 1$ is an integer. By the definition of oddness, this means that $5n^2 + n + 3$ is odd.

<u>Case 2: n is odd.</u> If n is even, then by the definition of an even integer, $n = 2a+1$ for some integer a. Then,

$$5n^2+n+3 = 5(2a+1)^2+(2a+1)+3 = 5(4a^2+4a+1)+2a+4 = 20a^2+22a+8+1 = 2(10a^2+11a+4)+1.$$

Since a is an integer, also $10a^2+11a+4$ is an integer, by Fact 2.1. Thus, we have shown that $5n^2+n+3 = 2k+1$ where $k = 10a^2 + 11a + 4$ is an integer. By the definition of oddness, this means that $5n^2 + n + 3$ is odd.

These two cases combine show that for any integer n, the result holds. □

Solution to Question 4.

Part (a). Assume that $m \mid n$. By the definition of divisibility, $n = md$ for some integer d. Thus, by squaring both sides, $n^2 = m^2d^2$. And since d is an integer, by Fact 2.1, $d \cdot d = d^2$ is an integer too.

We have shown that $n^2 = m^2k$ where $k = d^2$ is an integer. Thus, by the definition of divisibility, $m^2 \mid n^2$, as desired. □

Part (c). Assume that $m \mid n$ and $m \mid t$. By the definition of divisibility, $n = md$ and $t = m\ell$ for some integers d and ℓ. Thus,

$$n + t = md + m\ell = m(d + \ell).$$

And, since $d + \ell$ is also an integer by Fact 2.1, we have shown that $n + t = mk$ where $k = d + \ell$ is an integer. Therefore, by the definition of divisibility we have shown that $m \mid (n + t)$. □

Solution to Question 5.

Part (a). Assume that n is an integer. By Fact 2.1, n is either even or odd.

Case 1: n is even. If n is even, then by the definition of an even integer, $n = 2a$ for some integer a. Then,

$$1 + (-1)^n(2n - 1) = 1 + (-1)^{2a}(2(2a) - 1) = 1 + (4a - 1) = 4a.$$

We have shown that $1 + (-1)^n(2n - 1) = 4a$ where a is an integer, which by the definition of divisibility means 4 divides $1 + (-1)^n(2n - 1)$.

Case 2: n is odd. If n is odd, then by the definition of an odd integer, $n = 2a + 1$ for some integer a. Then,

$$1 + (-1)^n(2n - 1) = 1 + (-1)^{2a+1}(2(2a + 1) - 1) = 1 - (4a + 1) = -4a.$$

We have shown that $1+(-1)^n(2n-1) = 4(-a)$ where $-a$ is an integer, which by the definition of divisibility means 4 divides $1 + (-1)^n(2n - 1)$.

These two cases combine to show that for any integer n, the result holds. □

Part (b). Consider an arbitrary multiple of 4, which we write as $4k$ for an integer k.

Consider two cases. First, if $k > 0$, then note that by letting $n = 2k$, we have

$$1 + (-1)^n(2n - 1) = 1 + (-1)^{2k}(2(2k) - 1) = 1 + (4k - 1) = 4k.$$

That is, we have found a value of n for which $1 + (-1)^n(2n - 1) = 4k$.

If, on the other hand, we are considering a $4k$ for which $k \leq 0$, then note that by letting $n = -2k + 1$ (which is positive, since k is negative or zero) we have

$$1 + (-1)^n(2n - 1) = 1 + (-1)^{-2k+1}(2(-2k + 1) - 1) = 1 - (-4k + 1) = 4k.$$

That is, we have found a value of n for which $1 + (-1)^n(2n - 1) = 4k$.

In either case we have found a positive value of n for which $1 + (-1)^n(2n - 1)$ is equal to our arbitrary multiple of 4. This concludes the proof. □

Solution to Question 6.

(a) $q = 3$, $r = 2$.
(b) $q = 0$, $r = 5$
(c) $q = -4$, $r = 2$

Solution to Question 7. First, recall that finding the remainder is the same thing as determining what 4^{301} is congruent to modulo 17. Next, notice that $4^2 \equiv 16 \equiv -1 \pmod{17}$. Next, by applying Proposition 2.15 part (iii) (150 times),

$$\underbrace{4^2 \cdot 4^2 \cdot 4^2 \cdot \ldots \cdot 4^2}_{150 \text{ times}} \equiv \underbrace{(-1) \cdot (-1) \cdot (-1) \cdot \ldots \cdot (-1)}_{150 \text{ times}} \pmod{17}.$$

That is,

$$(4^2)^{150} \equiv (-1)^{150} \pmod{17},$$

which means that

$$4^{300} \equiv 1 \pmod{17}.$$

Next, notice that 4^{301} can be written like this:

$$4^{301} = 4^{300} \cdot 4^1.$$

Combining these and the arithmetic properties of modulo arithmetic, Proposition 2.15 part (iii),

$$4^{301} \equiv 4^{300} \cdot 4^1 \equiv 1 \cdot 4 \equiv 4 \pmod{17}.$$

And so, we have shown that $4^{301} \equiv 4 \pmod{17}$, which means that when 4^{301} is divided by 17, the remainder is 4. $\square$

Solution to Question 8. Part (a). Assume that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By the definition of the modulus,

$$m \mid (a-b) \qquad \text{and} \qquad m \mid (c-d).$$

Then, by the definition of divisibility,

$$a - b = mk \qquad \text{and} \qquad c - d = m\ell$$

for some integers k and ℓ. Subtracting these two equations,

$$(a-b) - (c-d) = mk - m\ell.$$

Regrouping,

$$(a-c) - (b-d) = m(k-\ell).$$

Since $k - \ell$ is an integer, by the definition of divisibility

$$m \mid \big[(a-c) - (b-d)\big],$$

which then by the definition of the modulus means that

$$a - c \equiv b - d \pmod{m},$$

completing the proof of part (b). $\square$

Part (b). Assume that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By the definition of the modulus,

$$m \mid (a-b) \qquad \text{and} \qquad m \mid (c-d).$$

Then, by the definition of divisibility,

$$a - b = mk \qquad \text{and} \qquad c - d = m\ell$$

for some integers k and ℓ. That is,

$$a = b + mk \qquad \text{and} \qquad c = d + m\ell$$

Multiplying these two equations,

$$\begin{aligned} ac &= (b + mk)(d + m\ell) \\ ac &= bd + mkd + m\ell b + m^2 k\ell \\ ac - bd &= m(kd + \ell b + mk\ell). \end{aligned}$$

Since $kd + \ell b + mk\ell$ is an integer, by the definition of divisibility

$$m \mid (ac - bd),$$

which then by the definition of the modulus means that

$$ac \equiv bd \pmod{m},$$

completing the proof of part (b). $\square$

Solution to Question 9. Assume that a is an integer and p and q are distinct primes. We first note that this implies that $\gcd(p, q) = 1$, which is the case by Lemma 2.17(a). Indeed, since q is a prime, 1 and q are the only positive numbers which divide it, and since p is neither of these, $p \nmid q$ and hence Lemma 2.17(a) tells use that $\gcd(p, q) = 1$.

Next, since the problem assumes that $p \mid a$, by the definition of divisibility we have $a = pk$ for some integer k. Since $q \mid a$ and $a = pk$, this means that $q \mid pk$. And since we already showed that $\gcd(p, q) = 1$, by Lemma 2.17(b) we deduce that $q \mid k$. By the definition of divisibility this means that $k = qt$ for some integer t.

Combining our work, we know that

$$a = pk = p(qt) = (pq)t,$$

which by the definition of divisibility means that $pq \mid a$, as desired. $\square$

Solution to Question 10. Since n is an integer, by Fact 2.1 n is either even or odd. Consider these two cases.

<u>Case 1: n is even.</u> If n is even, then by the definition of an even integer, $n = 2a$ for some integer a. Then,

$$n^2 = (2a)^2 = 4a^2.$$

Since a is an integer, also a^2 is an integer, by Fact 2.1. Thus, we have shown that $n^2 = 4k$ where $k = a^2$ is an integer. By the definition of divisibility, this means $4 \mid n^2$. This is equivalent to $4 \mid (n^2 - 0)$, which by the definition of the modulus means that $n^2 \equiv 0 \pmod 4$. Thus, in this case, we have proven the result.

<u>Case 2: n is odd.</u> If n is odd, then by the definition of an odd integer, $n = 2a + 1$ for some integer a. Then,

$$n^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 4(a^2 + a) + 1.$$

Since a is an integer, also $a^2 + a$ is an integer, by Fact 2.1. Thus, we have shown that $n^2 - 1 = 4k$ where $k = a^2 + a$ is an integer. By the definition of divisibility, this means $4 \mid (n^2 - 1)$. By the definition of the modulus, this means that $n^2 \equiv 1 \pmod 4$. Thus, in this case, we have proven the result.

These two cases combine to show that for any integer n, the result holds. $\square$