MATH 271 ASSIGNMENT 2 SOLUTIONS

1. (a) Show algebraically that $a^{n+1} - b^{n+1} = a(a^n - b^n) + b^n(a - b)$.

(b) Use part (a) to prove **using mathematical induction** (or well ordering) that $(a - b) \mid (a^n - b^n)$ for all integers a, b, n with $n \geq 1$.

(c) Use part (b) to prove that $11|(7^{271} + 4^{271})$.

(d) Prove part (b) again by proving that $a^n - b^n = (a - b)\sum_{i=0}^{n-1} a^{n-1-i}b^i$ for all integers $n \geq 1$, using telescoping. (See Example 4.1.10, page 205.)

(a) We get

$$a(a^n - b^n) + b^n(a - b) = a^{n+1} - ab^n + b^n a - b^{n+1} = a^{n+1} - b^{n+1}.$$

(b) We let a and b be arbitrary integers, and do induction on the integer n.

Basis step: When $n = 1$ the statement says $(a - b) \mid (a - b)$ which is clearly true for all integers a and b. [*Note*: this is true even if $a = b$, since we mentioned in class that, by the definition of divides, $0|0$ is true.]

Inductive step: Assume that $(a - b) \mid (a^k - b^k)$ for some integer $k \geq 1$. This means that $a^k - b^k = (a - b)S$ for some integer S. We want to prove that $(a - b) \mid (a^{k+1} - b^{k+1})$. Well,

$$\begin{aligned}
a^{k+1} - b^{k+1} &= a(a^k - b^k) + b^k(a - b) && \text{by part (a)}\\
&= a(a - b)S + b^k(a - b) && \text{by assumption}\\
&= (a - b)(aS + b^k)
\end{aligned}$$

where $aS + b^k$ is an integer, since $a, S, b \in \mathbb{Z}$ and k is a positive integer. Thus by definition, $(a - b) \mid (a^{k+1} - b^{k+1})$, which proves the inductive step.

Therefore by induction, $(a - b) \mid (a^n - b^n)$ for all integers a, b, n with $n \geq 1$.

(c) Since the statement in (b) is true for all integers a, b, n with $n \geq 1$, we can let $a = 7$, $b = -4$, and $n = 271$. Then the statement in (b) becomes $(7 - (-4)) \mid (7^{271} - (-4)^{271})$ which simplifies to $11|(7^{271} + 4^{271})$ (since 271 is odd).

(d) We get

$$\begin{aligned}
(a - b)\sum_{i=0}^{n-1} a^{n-1-i}b^i &= (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1})\\
&= (a - b)a^{n-1} + (a - b)a^{n-2}b + (a - b)a^{n-3}b^2 + \cdots + (a - b)b^{n-1}\\
&= a^n - ba^{n-1} + a^{n-1}b - a^{n-2}b^2 + a^{n-2}b^2 - a^{n-3}b^3 + \cdots + ab^{n-1} - b^n\\
&= a^n - b^n \qquad \text{because all the inside terms cancel out.}
\end{aligned}$$

Since $\sum_{i=0}^{n-1} a^{n-1-i}b^i$ is an integer (since a and b are integers), we get that $(a-b) \mid (a^n-b^n)$ by definition of divides.

Note: two special cases of this identity are the factoring formulas

$$a^2 - b^2 = (a - b)(a + b) \qquad \text{and} \qquad a^3 - b^3 = (a - b)(a^2 + ab + b^2).$$

2. The sequence $a_1, a_2, a_3, \ldots$ is defined by: $a_1 = 0$ and $a_{n+1} = a_n + 2n + 1$ for all integers $n \geq 1$.

   (a) Calculate a_2, a_3 and a_4.

   (b) Use part (a) (and more data if you need it) to guess a simple formula for a_n for all positive integers n.

   (c) **Use mathematical induction** (or well ordering) to prove that your guess in part (b) is correct.

   (d) Prove that a_n is composite for all integers $n \geq 3$.

   (a) We get

   - $a_2 = a_1 + 2 \cdot 1 + 1 = 0 + 2 + 1 = \mathbf{3}$,
   - $a_3 = a_2 + 2 \cdot 2 + 1 = 3 + 4 + 1 = \mathbf{8}$,
   - $a_4 = a_3 + 2 \cdot 3 + 1 = 8 + 6 + 1 = \mathbf{15}$.

   (b) From part (a), noticing that

   $$a_1 = 0 = 1^2 - 1, \qquad a_2 = 3 = 2^2 - 1, \qquad a_3 = 8 = 3^2 - 1, \qquad \text{and} \quad a_4 = 15 = 4^2 - 1,$$

   we might guess that $a_n = n^2 - 1$ for all positive integers n.

   (c) *Basis step*: When $n = 1$ our guess says that $a_1 = 1^2 - 1 = 0$, which is true.

   Inductive step: Assume that our guess is true when n equals some integer $k \geq 1$. In other words we assume that $a_k = k^2 - 1$. We want to prove that $a_{k+1} = (k+1)^2 - 1$. Well,

   $$\begin{aligned} a_{k+1} &= a_k + 2k + 1 \qquad \text{by the recursion} \\ &= (k^2 - 1) + 2k + 1 \qquad \text{by assumption} \\ &= (k^2 + 2k + 1) - 1 = (k+1)^2 - 1, \end{aligned}$$

   which proves the inductive step.

   Therefore by induction, $a_n = n^2 - 1$ is true for all integers $n \geq 1$.

   (d) From part (c), $a_n = n^2 - 1 = (n-1)(n+1)$. If $n \geq 3$ is an integer then both $n - 1$ and $n + 1$ are integers greater than 1. Therefore, by definition, a_n is composite if $n \geq 3$.

3. You are given the following "while" loop:

   [*Pre-condition*: m is a nonnegative integer, $a = 1$, $b = 1$, $i = 0$.]

   while $(i \neq m)$

   1. $a := a + 2b$
   2. $b := b - 2a$
   3. $i := i + 1$

   end while

   [*Post-condition*: $a = (-1)^m(1 - 4m)$.]

   Loop invariant $I(n)$ is: $i = n, \quad a = (-1)^n(1 - 4n), \quad b = (-1)^n(1 + 4n)$.

(a) Prove the correctness of this loop with respect to the pre- and post-conditions.

(b) Suppose the "while" loop is as above, with the same pre-condition, except that statements 1 and 2 are switched (so the new statements 1 and 2 are: 1. $b := b - 2a$, 2. $a := a + 2b$). Run through this new loop a few times to get data. Then find a post-condition that gives the final value of a, and an appropriate loop invariant, and prove the correctness of this new loop.

(a) We first need to check that the loop invariant holds when $n = 0$. But $I(0)$ says $i = 0$, $a = (-1)^0(1 - 4 \cdot 0) = 1$, and $b = (-1)^0(1 + 4 \cdot 0) = 1$, and these are all true by the pre-conditions.

So now assume that the loop invariant $I(k)$ holds for some integer $k \geq 0$ where $k < m$. We want to prove that $I(k+1)$ holds, that is, that the loop invariant will still hold after one more pass through the loop. So we are assuming that

$$i = k, \quad a = (-1)^k(1 - 4k), \quad b = (-1)^k(1 + 4k),$$

and we now go through the loop.

- Step 1:

$$\begin{aligned} a := a + 2b &= (-1)^k(1 - 4k) + 2(-1)^k(1 + 4k) \\ &= (-1)^k[1 - 4k + 2 + 8k] = (-1)^k(3 + 4k) \\ &= (-1)^k(-1 + 4 + 4k) = (-1)^k(-1 + 4(k + 1))(-1)^2 \\ &= (-1)^{k+1}(1 - 4(k + 1)), \end{aligned}$$

which agrees with the formula for a in $I(k + 1)$.

- Step 2:

$$\begin{aligned} b := b - 2a &= (-1)^k(1 + 4k) - 2(-1)^{k+1}(1 - 4(k + 1)) \\ &= (-1)^k[1 + 4k + 2(1 - 4k - 4)] = (-1)^k(1 + 4k + 2 - 8k - 8) \\ &= (-1)^k(-5 - 4k) = (-1)^{k+1}(5 + 4k) \\ &= (-1)^{k+1}(1 + 4(k + 1)), \end{aligned}$$

which agrees with the formula for b in $I(k + 1)$.

- Step 3: $i := i + 1 = k + 1$, which agrees with $I(k + 1)$.

Thus $I(k + 1)$ is true, as required.

Finally the loop stops when $i = m$, and we need to check that at that point the post-condition is satisfied. When $i = m$ it means that the loop invariant $I(m)$ must hold, so from $I(m)$ we know that $a = (-1)^m(1 - 4m)$, as required in the post-condition.

(b) If we set the variables to their pre-condition values of $a = 1$, $b = 1$ and $i = 0$, and run through the loop, the new values we get are

$$b = 1 - 2 \cdot 1 = -1, \quad a = 1 + 2(-1) = -1, \quad i = 0 + 1 = 1.$$

The next time through the loop we get

$$b = -1 - 2(-1) = 1, \quad a = -1 + 2 \cdot 1 = 1, \quad i = 1 + 1 = 2.$$

So the values of a and b are back to what they were at the beginning. Thus it certainly looks like the post-condition should be $a = (-1)^m$, and the loop invariant $I(n)$ should be: $i = n, \quad a = (-1)^n, \quad b = (-1)^n$. From the pre-condition, $I(0)$ is true. So assume that $I(k)$ holds for some integer $k \geq 0$ where $k < m$, and we want to prove that $I(k+1)$ holds. So we are assuming that

$$i = k, \quad a = (-1)^k, \quad b = (-1)^k,$$

and we now go through the loop.

- Step 1: $\quad b := b - 2a = (-1)^k - 2(-1)^k = -(-1)^k = (-1)^{k+1}$,
  which agrees with the formula for b in $I(k+1)$.
- Step 2: $\quad a := a + 2b = (-1)^k + 2(-1)^{k+1} = (-1)^k(1-2) = (-1)^{k+1}$,
  which agrees with the formula for a in $I(k+1)$.
- Step 3: $\quad i := i + 1 = k + 1$, which agrees with $I(k+1)$.

Thus $I(k+1)$ is true, as required.

Finally the loop stops when $i = m$, and then the loop invariant $I(m)$ must hold, so from $I(m)$ we know that $a = (-1)^m$ as required in the post-condition.