# MATH 13 HOMEWORK 3 ANSWER KEY

**Problem 3.1.1:** Since $17 \equiv 2(mod\ 5)$ and $2^2 \equiv -1(mod\ 5)$, we have

$$17^{251} \equiv 2^{251} \equiv 2 * 2^{250} \equiv 2 * (2^2)^{125} \equiv 2 * (-1)^1 25 \equiv -2(mod\ 5)$$

Now $23 \equiv 3 \equiv -2\ (mod\ 5)$, so

$$23^{12} \equiv (-2)^{12} \equiv ((-2)^2)^6 \equiv (-1)^6 \equiv 1\ (mod\ 5).$$

Now, $19 \equiv 4 \equiv -1(mod\ 5)$, so

$$19^{41} \equiv (-1)^{41} \equiv -1(mod\ 5)$$

Putting it all together, we have

$$17^{251} * 23^{12} - 19^{41} \equiv (-2) * 1 - (-1) \equiv -1(mod\ 5).$$

**Problem 3.1.6 (a,b,c):**

(a): We need to show that $7x \equiv 28(mod\ 42) \Rightarrow x \equiv 4(mod\ 6)$. Assume $7x \equiv 28(mod\ 42)$. Using Theorem 3.6, we get that

$$42|(7x - 28).$$

Since $42 = 7 * 6$ and $7x - 28 = 7(x - 4)$, the above can be written as

$$7 * 6|7(x - 4).$$

This means $7(x - 4) = 7 * 6 * k$ for some integer $k$. By cancellation, $x - 4 = 6 * k$; in other words,

$$6|(x - 4).$$

Applying Theorem 3.6 again, we get $x \equiv 4(mod\ 6)$ as desired.

(b): The question asks whether there is an $x$ such that $7x \equiv 28(mod\ 42)$ and $x \equiv 4(mod\ 42)$. The answer is YES. $x = 4$ satisfies the requirement.

(c): It is NOT always the case that for any $x$, if $7x \equiv 28(mod\ 42)$, then $x \equiv 4(mod\ 42)$. For example if $x = 10$, then $7x = 70 \equiv 28(mod\ 42)$, but $\neg(10 \equiv 4(mod\ 42))$.

**Problem 3.1.1 and 3.1.2 (b):** The $gcd(100, 36) = 4$. And $4 = 4 * 100 - 11 * 36$. This is just using the Euclidean algorithm. I leave the details to you.

**Problem 3.2.9:** Let $m, n$ be arbitrary integers.

$(\Rightarrow)$ : Assume $gcd(m, n) = 1$. Then by Corollary 3.12, there are integers $x, y$ such that $gcd(m, n) = mx + ny$. Since $gcd(m, n) = 1$, we have $1 = mx + ny$.

$(\Leftarrow)$ : Assume there are integers $x, y$ such that $mx + ny = 1$. We want to show $gcd(m, n) = 1$.

Let $d = gcd(m, n)$. So there are integers $k, l$ such that $m = k * d$ and $n = l * d$. So $mx + ny = d * (kx + ly)$. This implies $d|(mx + ny)$. So $d|1$. The only positive integer that divides 1 is 1 itself. Hence $d = 1$ as desired.

**Problem 3.2.11:** We will apply the Euclidean algorithm to find $gcd(12n + 5, 5n + 2)$. But first, we need some observation:

$$12n + 5 \geq 5n + 2 \Leftrightarrow 7n \geq -3 \Leftrightarrow n \geq -3/7.$$

Since $n$ is an integer, $n \geq -3/7 \Leftrightarrow n \geq 0$. So we have that

$$12n + 5 \geq 5n + 2 \Leftrightarrow n \geq 0.$$

So for any integer $n \geq 0$, we know $12n + 5 \geq 5n + 2$, applying the Euclidean algorithm:

$$12n + 5 = 2(5n + 2) + (2n + 1) \; 5n + 2 = 2(2n + 1) + n$$

Now if $n = 0$, then we know $12n + 5 = 5$ and $5n + 2 = 2$ and $gcd(2, 5) = 1$, so we're done. If $n > 0$, we continue with the Euclidean algorithm

$$2n + 1 = 2(n) + 1 \; n = n(1) + 0$$

So we again conclude that $1 = gcd(12n + 5, 5n + 2)$.

That takes care of the case $n \geq 0$. Now suppose $n < 0$ (so the absolute value $|n| > 0$), so we know $12n + 5 < 5n + 2 < 0$, but then $|12n + 5| > |5n + 2| > 0$. Since $gcd(12n + 5, 5n + 2) = gcd(|12n + 5|, |5n + 2|) = gcd(12|n| + 5, 5|n| + 2)$, we apply the Euclidean algorithm in the previous argument to $12|n| + 5$ and $5|n| + 2$ and conclude again $gcd(12|n| + 5, 5|n| + 2) = 1$.