Math 311, Quiz 3

Name:_____

Instructions: Clearly answer each of the questions below. Remember to check the back side – if blank, you can use it for scrap work. Use full sentences and proper grammar. Show your work and any formulas you employ. Simplify all answers as far as possible. Box your answers when appropriate.

1. What is a congruence class $[a]_n$?

   Answer: *A congruence class $[a]_n$ is the set of all integers having the same remainder as a after division by n.*

2. Find $[9]_{49}^{-1}$ using the matrix GCD method, if it exists.

   Answer:

$$\left[\begin{array}{cc|c} 1 & 0 & 49 \\ 0 & 1 & 9 \end{array}\right]$$

$$\left[\begin{array}{cc|c} 0 & 1 & 9 \\ 1 & -5 & 4 \end{array}\right]$$

$$\left[\begin{array}{cc|c} 1 & -5 & 4 \\ -2 & 11 & 1 \end{array}\right]$$

$$\left[\begin{array}{cc|c} -2 & 11 & 1 \\ 9 & -49 & 0 \end{array}\right]$$

   So $-2(49) + 11(9) = 1$, or in congruence classes, $[-2(49) + 11(9)]_{49} = [11]_{49}[9]_{49} = [1]_{49}$, which means $[9]_{49}^{-1} = [11]_{49}$

3. Find $[6]_{26}^{-1}$ using the matrix GCD method, if it exists.

   Answer: *Does not exist, since* $\gcd(6, 26) = 2 > 1$.

4. Find $[5]_9[7]_9 + [3]_9$.

   Answer: $[5]_9[7]_9 + [3]_9 = [35]_9 + [3]_9 = [38]_9 = [36 + 2]_9 = [2]_9$

5. How would you know if a congruence class $[a]_n$ is a zero-divisor?

   Answer: *A $[a]_n$ is a zero-divisor congruence class if it is not equal to $[0]_n$ and there is some other congruence class $[b]_n \neq [0]_n$ such that $[a]_n[b]_n = [0]_n$. $[a]_n$ will be a zero-divisor if and only if $\gcd(a, n) > 1$.*

6. Give reasons for each of the following proof steps. Let's prove that if $[a]_n$ is invertible, then $[a]_n$ is not a zero-divisor. Suppose that there is some congruence class $[z]_n$ such that $[a]_n[z]_n = [0]_n$.

   (a) There is a congruence class $[i]_n$ such that $[i]_n[a]_n = [1]_n$, because ...

   Answer: *of the Definition of an invertible congruence class.*

   (b) We can change $[a]_n[z]_n = [0]_n$ into $[i]_n[a]_n[z]_n = [i]_n[0]_n$ by ...

   Answer: *the properties of multiplication.*

   (c) We know $[i]_n[0]_n = [0]_n$ because ...

   Answer: *of the properties of $[0]_n$ multiplication.*

   (d) On the left side, we know $[i]_n[a]_n[z]_n = [1]_n[z]_n$ because ...

   Answer: *of the definition of inverses (or substitution)*

   (e) and then $[1]_n[z]_n = [z]_n$ because ...

   Answer: *of the properties of $[1]_n$ multiplication*

   (f) So we determine that $[z]_n = [0]_n$ by ...

   Answer: *substitution into the left and right sides of $[i]_n[a]_n[z]_n = [i]_n[0]_n$.*

   (g) Then the only congruence class we can multiply $[a]_n$ by to get $[0]_n$ is $[0]_n$. We conclude that $[a]_n$ is not a zero-divisor because of ...

   Answer: *the definition of zero-divisors.*