Name: ______________________________ Score (Out of 8 points):

A non-programmable, non-scientific calculator may be used.

1. (a) [2 points] Find all congruences classes x modulo 14 that satisfy the equation

$$4x \equiv 10 \pmod{14}$$

Because $d = \gcd(4, 14) = 2$ and $2 \mid 12$, we expect there to be $d = 2$ solutions. To find these we divide through by $d = 2$:

$$\begin{aligned} 2x &\equiv 5 \pmod{7} \\ 2x &\equiv 12 \pmod{7} \qquad \text{Since } \gcd(7,2) = 1, \text{ we can divide by 2.} \\ x &\equiv 6 \pmod{7} \end{aligned}$$

Thus the two solutions modulo 14 are the classes $[6]$ and $[6 + 7] = [13]$.

(b) [3 points] Find all congruence classes x modulo $126 = (14)(9)$ that simultaneously satisfy the following equations:

$$\begin{aligned} 4x &\equiv 10 \pmod{14} \\ x &\equiv 5 \pmod{9} \end{aligned}$$

From part (a), we know the solutions to the first equation are $[6]$ and $[13]$. Thus we need to find all solutions to the two simultaneous systems:

$$\begin{aligned} x &\equiv 6 \pmod{14} \\ x &\equiv 5 \pmod{9} \end{aligned} \qquad\qquad \begin{aligned} x &\equiv 13 \pmod{14} \\ x &\equiv 5 \pmod{9} \end{aligned}$$

By the Chinese Remainder Theorem, each of these systems has precisely one solution modulo 126, giving two solutions total. To find the solutions, we first use the Euclidean algorithm to find $u, v \in \mathbb{Z}$ such that $14u + 9v = 1$.

$$\begin{aligned} 14 &= 9 + 5 \\ 9 &= 5 + 4 \\ 5 &= 4 + 1 \end{aligned} \qquad\qquad \begin{aligned} 1 &= 5 - 4 \\ 1 &= 5 - (9 - 5) \\ 1 &= 2(5) - (9) \\ 1 &= 2(14 - 9) - (9) \\ 1 &= 2(14) + (-3)(9) \end{aligned}$$

This gives the two solutions

$$(5)(2)(14) + (6)(-3)(9) = -22 \equiv 104 \pmod{126}$$

$$(5)(2)(14) + (13)(-3)(9) = -211 \equiv 41 \pmod{126}$$

and we conclude that the solutions are the classes are $[104]$ and $[41]$ modulo 126.

 The quiz continues on the back of the page.

2. [3 points] Suppose that $\gcd(m, n) = d$. Explain why, if a and b are **not** congruent modulo d, the following system of congruences has no solutions.

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

Suppose that x is an integer such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

By a result from Homework #1, since $d \mid m$ we can further reduce congruence modulo m to congruence classes modulo d. We must have $x \equiv a \pmod{d}$. Similarly $d \mid n$ so we must have $x \equiv b \pmod{d}$.

This implies that $a \equiv b \pmod{d}$. If a and b are not congruent modulo d, then this is a contradiction, and there can be no such solution x.