Name: Solutions

Directions: Show all work. No credit for answers without work.

1. [**3 points**] Give the addition and multiplication tables for $\mathbb{Z}_5$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

2. [**2 parts, 2 points each**] Compute the following. Your answer should be an integer in the set $\{0, 1, \ldots, m-1\}$, where m is the modulus in the given problem.

(a) $297 + 561 \pmod{48}$

$297 = (6)(48) + 9$, $297 \equiv 9 \pmod{48}$

$561 = (11)(48) + 33$, $561 \equiv 33 \pmod{48}$

$$297 + 561 \equiv 9 + 33 \pmod{48}$$
$$\equiv \boxed{42}$$

(b) $136 \cdot (-524) \pmod{87}$

$136 = (1)(87) + 49$ $\quad 136 \equiv 49 \pmod{87}$

$-524 = (-6)(87) - 2$ $\quad -524 \equiv -2 \pmod{87}$

$$136 \cdot (-524) \equiv (49) \cdot (-2) \pmod{87}$$
$$\equiv -98$$
$$\equiv -11$$
$$\equiv \boxed{76}$$

3. Let $a, b, c, m \in \mathbb{Z}$ with $m \geq 1$. X

(a) [**1 point**] According to the definition, what does $a \equiv b \pmod{m}$ mean?

It means $m \mid b-a$ or $b-a = km$ for some $k \in \mathbb{Z}$.

(b) [**2 points**] Prove that if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Since $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, we know that

$b - a = k_1 m$ and $c - b = k_2 m$ for some $k_1, k_2 \in \mathbb{Z}$.

Adding these gives $(c-b) + (b-a) = k_2 m + k_1 m$, or $c - a = (k_2 + k_1) m$.

Since $m \mid c - a$, it follows that $a \equiv c \pmod{m}$. ∎