1. *A grocer orders apples and oranges at a total cost of \$8.39. If apples cost 25 cents each and oranges cost 18 cents each, how many of each type of fruit did the grocer order? Is there more than one possibility? Explain.*

Let a denote the number of ordered apples and b denote the number of ordered oranges. We are looking for a nonnegative integer solution to the equation $25a + 18b = 839$. Since $(25, 18) = 1$ and 839 is a multiple of 1, we know that infinitely many integer solutions exist, but we need to see if there is a nonnegative integer solution available.

By inspection, observe that $25 \cdot (-5) + 18 \cdot 7 = 1$. Multiply through by 839 to find that $25 \cdot (-4195) + 18 \cdot (5873) = 839$. We know that every solution to $25a + 18b = 839$ then has the form $a = -4195 + 18k$ and $b = 5873 - 25k$. To find a nonnegative solution, we need $0 \leqslant a = -4195 + 18k$, implying that $k \geqslant \frac{4195}{18} \approx 233.05$ and we need $0 \leqslant b = 5873 - 25k$ implying that $k \leqslant \frac{5873}{25} \approx 234.92$. The only way for k to satisfy these constraints (while being an integer) is if $k = 234$, implying that $a = 17$ and $b = 23$ is the only nonnegative solution to $25a + 18b = 839$. Therefore, the grocer must have ordered 17 apples and 23 bananas.

2. *Define the set*

$$\mathbb{Z} \big/ m\mathbb{Z} := \{0, 1, 2, \ldots, m-1\}$$

(pronounced "zee mod m zee" in America and "zed mod m zed" in some other parts of the English-speaking world). For any $a, b \in \mathbb{Z} / m\mathbb{Z}$, define $a+b$ to be the unique element in $\mathbb{Z} / m\mathbb{Z}$ which is congruent to $a+b$ (usual addition in $\mathbb{Z}$) modulo m. Define $a \cdot b$ to be the unique element in $\mathbb{Z} / m\mathbb{Z}$ which is congruent to ab (usual multiplication in $\mathbb{Z}$) modulo m.

(a) *Fill out the following table of addition for $\mathbb{Z} / 5\mathbb{Z}$. In the row corresponding to a and column corresponding to b, put $a+b$. You can just fill out the table, you don't have to show work here.*

$+$	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

(b) *Fill out the following table of multiplication for $\mathbb{Z} / 5\mathbb{Z}$. In the row corresponding to a and column corresponding to b, put $a \cdot b$. You can just fill out the table, you don't have to show work here.*

$\cdot$	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

3. *Show that if* $a \equiv b \mod m$ *and* $d \mid m$*, then* $a \equiv b \mod d$*. Show that it is not the case that if* $a \equiv b \mod d$*, then* $a \equiv b \mod kd$*.*

   Suppose that $a \equiv b \mod m$ and $d \mid m$. Then there exist integers ℓ and k so that $a - b = m\ell$ and $dk = m$. Then we have $a - b = m\ell = dk\ell$, implying that $a - b$ is a multiple of d. Hence, $a \equiv b \mod d$.

   To see that the converse is not true, note that $2 \equiv 4 \mod 2$, but $2 \not\equiv 4 \mod 4$.

4. *Suppose that $a, b, c, d, m \in \mathbb{Z}$ with $a \equiv b \mod m$ and $c \equiv d \mod m$. Show that $ac \equiv bd \mod m$.*

Since $a \equiv b \mod m$ and $c \equiv d \mod m$, there exist $k, \ell \in \mathbb{Z}$ with $a - b = m\ell$ and $c - d = mk$. Then

$$ac - bd = a(d + mk) - bd = (a - b)d + amk = m\ell d + amk = m(\ell d + ak)$$

and hence, $ac - bd$ is a multiple of m, so $ac \equiv bd \mod m$.

5. *Suppose that $a, b, k, m \in \mathbb{Z}$ with $k \geqslant 0$ and $m \geqslant 1$. Show that if $a \equiv b \mod m$, then $a^k \equiv b^k \mod m$. You may use the result of the previous problem even if you were unable to prove it.*

We prove this by induction on k. Note that for $k = 0$, the claim is trivial since $1 \equiv 1 \mod m$. Suppose that $a^{k-1} \equiv b^{k-1} \mod m$. Then by the previous problem, since $a \equiv b \mod m$, we can multiply the left-hand side of the congruence $a^{k-1} \equiv b^{k-1} \mod m$ by a and we can multiply the right-hand side of the same congruence by b. But then $a^k \equiv b^k \mod m$.

Hence, by induction, $a^k \equiv b^k \mod m$ for all $k \geqslant 0$.

6. *Show that, for $n \geqslant 0$,*

$$7^n \equiv \begin{cases} 1 \mod 100 & \text{if } n \equiv 0 \mod 4 \\ 7 \mod 100 & \text{if } n \equiv 1 \mod 4 \\ 49 \mod 100 & \text{if } n \equiv 2 \mod 4 \\ 43 \mod 100 & \text{if } n \equiv 3 \mod 4 \end{cases}$$

Begin by writing $n = 4q + r$ where $q, r \in \mathbb{Z}$ with $0 \leqslant r < 3$ using Euclidean division and observe that this implies that $n \equiv r \mod 4$. Then note that $7^n = (7^4)^q \cdot 7^r = 2401^q \cdot 7^r$. Since $2401 \equiv 1 \mod 100$, the previous problem indicates that $2401^q \equiv 1^q \equiv 1 \mod 100$ and hence,

$$7^n \equiv 2401^q \cdot 7^r \equiv 7^r \mod 100$$

Since $0 \leqslant r < 3$, we find that 7^n only has four possible values mod 100:

If $n \equiv 0 \mod 4$, then $7^n \equiv 7^0 \equiv 1 \mod 100$. If $n \equiv 1 \mod 4$, then $7^n \equiv 7^1 \equiv 7 \mod 100$. If $n \equiv 2 \mod 4$, then $7^n \equiv 7^2 \equiv 49 \mod 100$. Finally, if $n \equiv 3 \mod 4$, then $7^n \equiv 7^3 \equiv 43 \mod 100$.