3.24 Theorem. Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Then

1. The congruence $ax \equiv m \pmod{n}$ is solvable in integers if and only if $(a, n)|b$;

2. If x_0 is a solution to the congruence $ax \equiv b \pmod{n}$, then all solutions are given by

$$x_0 + \left(\frac{n}{(a,n)}m\right) \pmod{n}$$

for $m = 0, 1, 2, ..., (a, n) - 1$; and

3. If $ax \equiv b \pmod{n}$ has a solution, then there are exactly (a, n) solutions in the canonical complete residue system modulo n.

Proof. 1. This is exactly Theorem 3.20.

2. Let $x = x_0$ be an integer solution to $ax \equiv b \pmod{n}$. By Theorem 1.53, all solutions are given by $x = x_0 + \frac{nk}{(a,n)}$ for some $k \in \mathbb{Z}$. We want to show $x_0 + \frac{nk}{(a,n)} \equiv x_0 + \frac{nm}{(a,n)} \pmod{n}$ for some $m = 1, 2, ..., (a, n) - 1$. Applying the division algorithm on k by (a, n) gives $k = (a, n)q + m$. Thus,

$$\begin{aligned}
x_0 + \frac{nk}{(a,n)} &\equiv x_0 + \frac{n[(a,n)q + m]}{(a,n)} \\
&\equiv x_0 + nq + \frac{nm}{(a,n)}, \text{ and since } nq \equiv 0 \pmod{n}, \\
&\equiv x_0 + \frac{nm}{(a,n)} \pmod{n}.
\end{aligned}$$

Thus, all solutions are given by $x_0 + \left(\frac{n}{(a,n)}m\right) \pmod{n}$ for $m = 0, 1, 2, ..., (a, n) - 1$.

3. Let $ax \equiv b \pmod{n}$ have a solution. We want to show there are exactly (a, n) solutions in the canonical complete residue system modulo n. Suppose not. That is, let $x_0 + \frac{nm}{(a,n)} \equiv x_0 + \frac{nk}{(a,n)} \pmod{n}$ where $k \neq m$ and $0 \leq k < m \leq (a, n) - 1$. Thus,

$$
\begin{aligned}
x_0 + \frac{nm}{(a,n)} &\equiv x_0 + \frac{nk}{(a,n)} \pmod{n}, \\
\frac{nm}{(a,n)} &\equiv \frac{nk}{(a,n)} \pmod{n}.
\end{aligned}
$$

This implies

$$
\begin{aligned}
&n \left| \left[\frac{nk}{(a,n)} - \frac{nk}{(a,n)} \right] \right. \\
&n | \frac{n}{(a,n)}(m-k).
\end{aligned}
$$

Some things to observe,

$$0 \leq k < m \leq (a,n) - 1 < (a,n) \leq n.$$

One of the properties of divisibility says for n to divide $\frac{n}{(a,n)}(m-k) > 0$, the condition $n \leq \frac{n}{(a,n)}(m-k)$ must occur. Observing the above inequality, we find

$$m - k \leq (a,n) - 1.$$

Thus,

$$\frac{n}{(a,n)}(n-k) \leq \frac{n}{(a,n)}[(a,n)-1] = n - \frac{1}{(a,n)} < n.$$

Since $n - \frac{n}{(a,n)}$ is less than n, we have a contradiction. Thus, if $ax \equiv b \pmod{n}$ has a solution, then there are exactly (a,n) solutions in the canonical complete residue system modulo n. $\square$