3.20 Theorem. Let $a, b, n \in \mathbb{Z}$ with $n > 0$. The equation $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n)|b$.

Proof. Let $ax \equiv b \pmod{n}$ be given such that it has a solution. By Theorem 3.19, there exists $x, y \in \mathbb{Z}$ such that $ax + ny = b$. By Theorem 1.48, $(a, n)|b$.

Let $(a, n)|b$ be given. By Theorem 1.48, there exists integers x, y such that $ax + ny = b$. By Theorem 3.19, $ax \equiv b \pmod{n}$. □