

**3.19 Theorem.** Let  $a, b$ , and  $c$  be integers with  $n > 0$ . Show that  $ax \equiv b \pmod{n}$  has a solution if and only if there exist integers  $x, y$  such that  $ax + ny = b$ .

**Proof.** Let  $ax \equiv b \pmod{n}$  be given such that a solution exists. By definition,  $ax - b = nk$  for  $k \in \mathbb{Z}$ . Rearranging,  $ax + ny = b$  where  $y = -k$ . Thus,  $ax + ny = b$  has a solution. Now let  $x, y \in \mathbb{Z}$  be given such that  $ax + ny = b$ . Rearranging,  $ax - b = -ny$ . Substituting  $-y = t$  for  $t \in \mathbb{Z}$ ,  $ax - b = nt$ . By definition,  $ax \equiv b \pmod{n}$ . Thus,  $ax \equiv b \pmod{n}$  has a solution if and only if there exist integers  $x, y$  such that  $ax + ny = b$ .  $\square$