

**1.45 Theorem.** Let  $a, b, c, n \in \mathbb{Z}$  with  $n > 0$ . If  $ac \equiv bc \pmod{n}$  and  $(c, n) = 1$ , then  $a \equiv b \pmod{n}$ .

**Proof.** Let  $a, b, c, n \in \mathbb{Z}$  with  $n > 0$  be given such that  $ac \equiv bc \pmod{n}$  and  $(c, n) = 1$ . By definition,  $n \mid (ac - bc)$ . Factoring  $c$ ,

$$n \mid c(a - b).$$

By Theorem 1.41, since  $(c, n) = 1$ ,  $n \mid (a - b)$ , and by definition,  $a \equiv b \pmod{n}$ .  $\square$