

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

Proof. Let $a \equiv b \pmod{n}$ with $(a, n) = 1$. By definition, $a = nk + b$ for some $k \in \mathbb{Z}$. Since $(a, n) = 1$, by Theorem 1.38, there exists $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Substituting for a ,

$$\begin{aligned} 1 &= x(nk + b) + by \\ &= nkx + bx + by \\ &= b(x + y) + n(kx). \end{aligned}$$

By CPI, let integers $x' = x + y$ and $y' = kx$ such that $bx' + ny' = 1$. By Theorem 1.39, $(b, n) = 1$. Thus, if $a \equiv b \pmod{n}$, then $(b, n) = 1$, provided $n > 0$ and $(a, n) = 1$. \square