4.38 Theorem. Let p be a prime and let a and b be integers such that $1 < a, b < p - 1$ and $ab \equiv 1 \pmod{p}$. Then $a \neq b$.

Proof. Suppose not. That is suppose $a = b$. Since $a = b$, $ab \equiv 1 \pmod{p}$ is equivalent to $a^2 \equiv 1 \pmod{p}$. By definition,

$$\begin{aligned} p|&a^2 - 1 \\ &|(a-1)(a+1). \end{aligned}$$

By Theorem 2.27, $p|a-1$ or $p|a+1$. Notice $0 < a-1 < p-2$ and $2 < a+1 < p$. This is a contradiction of p being smaller than any natural number it divides. Thus, if p is prime and $a, b \in \mathbb{Z}$ such that $1 < a, b < p-1$ and $ab \equiv 1 \pmod{p}$, then $a \neq b$. $\square$