4.36 Theorem. Let p be a prime and $a \in \mathbb{Z}$ where $1 \leq a < p$. Then there exists a unique integer $b < p$ such that $ab \equiv 1 \pmod{p}$.

Proof. Since $(a, p) = 1$, by Theorem 1.38, there exists $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Applying TDA on x with p, $x = pq + b$ for some $q, b \in \mathbb{Z}$ and $0 \leq b \leq p - 1$. Substitution for x,

$$\begin{aligned} a(pq + b) + py &= 1, \\ apq + ab + py &= 1, \\ ab - 1 &= -py - apq, \\ ab - 1 &= p(-y - aq). \end{aligned}$$

By CPI, let $-y - aq = q' \in \mathbb{Z}$ such that $ab - 1 = pq'$. Thus, by definition, $ab \equiv 1 \pmod{p}$. Furthermore, let $b' \in \mathbb{Z}$ where $1 \leq b' < p$, and WLOG $b' < b$, such that $ab \equiv 1 \pmod{p}$ and $ab' \equiv 1 \pmod{p}$. By transitivity, $ab \equiv ab' \pmod{p}$. By definition,

$$ab - ab' = pk$$

for some $k \in \mathbb{Z}$. We find,

$$a(b - b') = pk.$$

This implies $p | a(b - b')$. Since $p \not| a$, $p | b - b'$. Since $1 \leq b, b' < p$ implies $0 \leq b - b' < p$, p can only divide if $b - b' = 0$. Thus, b and b' are the same, i.e., $b = b'$. Therefore, there exists a unique integer $b < p$ such that $ab \equiv 1 \pmod{p}$. $\square$