4–4, #8 Show that an inverse of $a$ modulo $m$, where $a$ is an integer and $m > 2$ is a positive integer, does not exist if $\gcd(a, m) > 1$.

Here I'll present two proofs of this problem. The first one uses some nice tools that we have at our disposal, and the second one is somewhat shorter.

Proof (I): If $k \geq 1$ is an integer, consider the sets

\[ A = \{d : d|a \land d|m\}, \quad \text{and} \quad B = \{d : d|ak \land d|m\}. \]

If $d \in A$, then $d \in B$ since $d|a$ implies $d|ak$. Therefore $A \subseteq B$, and we can conclude that $\gcd(a, m) \leq \gcd(ak, m)$, since the gcd is defined as the largest member of each of these sets. Therefore, for every positive integer $k$, we have

\[ 1 < \gcd(a, m) \leq \gcd(ak, m). \]

Suppose, for the sake of a contradiction, that $k \geq 1$ were an inverse of $a$. This means that $ak \equiv 1 \pmod{m}$. This relationship tells us that there exists a $q \in \mathbb{Z}$, with

\[ ak = qm + 1. \]

Given this relationship, we know that

\[ 1 < \gcd(ak, m) = \gcd(m, 1) = 1. \]

This is a contradiction, and therefore no such $k$ can exist. \hfill \Box

Actually, here is a much shorter proof.

Proof (II): In this proof, we'll prove the contrapositive. That is, if $a$ has an inverse, then $\gcd(a, m) = 1$.

Suppose $ak \equiv 1 \pmod{m}$. Then, there exists, $q$ such that

\[ ak = qm + 1. \]

With $d = \gcd(a, m)$, we know that $d$ divides both $a$ and $m$. Therefore, $d$ divides any linear combination of $a$ and $m$, and hence $d$ divides

\[ 1 = ak - qm. \]

Since $d$ divides 1, the largest it could possibly be is the number 1 itself.