Prove: if \( a, m \) are integers, \( m > 0 \), and \( \text{GCD}(a, m) = 1 \), then there exists an integer \( a' \) such the \( a \cdot a' \equiv 1 \pmod{m} \).

Proof
Since \( \text{GCD}(a, m) = 1 \), there are integers \( s, t \) such that \( sa + tm = 1 \).
Let \( a' = s \).

Then
\[
a \cdot a' + tm = 1
\]
so
\[
a \cdot a' - 1 = -tm
\]

This shows that \( m \mid (a \cdot a' - 1) \), so, according to the definition of modular congruence, \( a \cdot a' \equiv 1 \pmod{m} \).