Discrete Math Challenge HW 7 (2 points)

In class, we proved that for any $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, if $\gcd(a, m) = 1$ then a has a multiplicative inverse modulo m, that is,

$$\forall a : \mathbb{Z}.\ \forall m : \mathbb{Z}^+.\ (\gcd(a, m) = 1) \to (\exists b : \mathbb{Z}.\ ab \equiv_m 1)\,.$$

It turns out this is actually an if and only if. Prove the other direction, that is,

$$\forall a : \mathbb{Z}.\ \forall m : \mathbb{Z}^+.\ (\exists b : \mathbb{Z}.\ ab \equiv_m 1) \to (\gcd(a, m) = 1).$$