Page 24 Exercise 11

Let n and a be positive integers and let d = gcd(a, n). Show that the equation ax ≡ 1 mod n has a solution iff d = 1. (This exercise is referred to in Chapter 2.)

Let a, n $\in \mathbb{Z}^+$.
Let d = gcd(a, n)
$\longrightarrow$
Want to show: ax ≡ 1 mod n $\Rightarrow$ d = 1
Suppose ax ≡ 1 mod n.
Then $\exists$ t $\in \mathbb{Z}$ st
tn = 1 − ax
tn + xa = 1
Since $\exists$ t, x $\in \mathbb{Z}$ such that tn + xa = 1,
a and n are relatively prime.
Therefore, gcd(a, n) = d = 1.
$\longleftarrow$
Want to show: d = 1 $\Rightarrow$ ax ≡ 1 mod n
Suppose d = 1.
Then gcd(a, n) = 1.
Thus, $\exists$ t, x $\in \mathbb{Z}$ such that tn + ax = 1.
tn + ax = 1
tn = 1 − ax
Thus, t is a possible solution to ax ≡ 1 mod n