Page 24 Exercise 11

Let n and a be positive integers and let d = gcd(a, n). Show that the equation ax mod n = 1 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 mod n = 1 $\Rightarrow$ d = 1

Suppose ax mod n = 1.

$\longleftarrow$

Want to show: d = 1 $\Rightarrow$ ax mod n = 1 Suppose d = 1.