

(Q4)

(a)

*Proof.* By earlier proof,  $\gcd(a, n) = 1 \implies \exists x \in \mathbb{Z} : [a] \cdot [x] = [1]$  in  $\mathbb{Z}_n$ .

We now seek to prove the converse:

$$\exists x \in \mathbb{Z}_n : [a] \cdot [x] = [1] \implies \gcd(a, n) = 1$$

Let  $[a] \cdot [x] = [1]$  in  $\mathbb{Z}_n$ . Then by definition of congruence modulo  $n$ , we have

$$ax \equiv 1 \pmod{n} \implies n \mid 1 - ax \implies \exists y \in \mathbb{Z} : yn = 1 - ax$$

Then by Bézout's Identity:

$$\exists x, y \in \mathbb{Z} : ax + yn = 1 \implies \gcd(a, n) = 1$$

■

Since both directions have been proven, this statement is if and only if.

(b) Since  $\forall n \in \mathbb{N}, \mathbb{Z}_n$  fulfills all the field axioms except for that of the multiplicative identity, if every nonzero element of  $\mathbb{Z}_n$  has a multiplicative identity,  $\mathbb{Z}_n$  is a field. This occurs iff  $n$  is prime.