

(Q6)

(a)

Proof. We have that for any \mathbb{Z}_n :

$$\underbrace{[1] + [1] + \dots + [1] + [1]}_{x \text{ times}} = [x]$$

Then in \mathbb{Z}_p :

$$\underbrace{[1] + [1] + \dots + [1] + [1]}_{p \text{ times}} = [p] = [0]$$

Which means $\text{char}(\mathbb{Z}_p) = p$. ■

(b)

Proof. Let \mathbb{F} be a field. Suppose for the sake of contradiction that $p = \text{char}(\mathbb{F}) \neq 0$ and p is composite. Then

$$\exists x, y \in \mathbb{Z} : xy = \text{char}(\mathbb{F}) \implies xy \cdot 1_{\mathbb{F}} = (x \cdot 1_{\mathbb{F}}) \cdot (y \cdot 1_{\mathbb{F}}) = 0$$

which in turn means $x \cdot 1_{\mathbb{F}} = 0$ or $y \cdot 1_{\mathbb{F}} = 0$.

Since $x, y < p$, this contradicts the assumption that $p = \text{char}(\mathbb{F})$, so p has to be prime.

For fields that have characteristic 0, consider infinite fields such as \mathbb{Q} or \mathbb{R} . In such fields, repeatedly adding 1 to itself will never yield 0, thus fields can have characteristic 0. If $\text{char}(\mathbb{F}) \neq 0$, then $\text{char}(\mathbb{F})$ is prime. ■