

2.3.9

$$\begin{aligned}
 & a \text{ is a unit in } \mathbb{Z}_n \\
 & \exists b \in \mathbb{Z}_n \quad ab \equiv 1 \pmod{n} \\
 & \quad n \mid ab - 1 \\
 & \quad \Downarrow \\
 & \exists k \in \mathbb{Z} \quad ab - 1 = nk \\
 & \quad ab - nk = 1 \\
 & \quad ab + n(-k) = 1 \\
 & \quad \gcd(a, n) = 1
 \end{aligned}$$

$$\begin{aligned}
 & \forall c \in \mathbb{Z}_n \setminus \{0\} \quad ac \neq 0 \\
 & \quad \Updownarrow \\
 & \nexists c \in \mathbb{Z}_n \quad ac \equiv 0 \\
 & \quad \uparrow \\
 & (c \in \mathbb{Z}_n \text{ and } ac \equiv 0) \Rightarrow (c \equiv 0)
 \end{aligned}$$

$$\begin{aligned}
 & \gcd(a, n) = 1 \\
 & \exists k \in \mathbb{Z}, r \in \mathbb{Z}_n \quad nk + r = c \\
 & \quad \exists m \in \mathbb{Z} \quad ac = mn \\
 & \quad a(nk + r) = mn \\
 & \quad ar = n(m - ak) \\
 & \quad \quad n \mid ar \\
 & \quad \gcd(a, n) = 1 \\
 & \quad n \mid r \text{ by Euclid's lemma} \\
 & \quad \quad r = 0 \\
 & \quad \quad c = nk \\
 & \quad \quad c \equiv 0
 \end{aligned}$$