Definition. Let $n \geq 2$ be a positive integer. Then

$$U(n) := \{a \in \{0, \ldots, n-1\} : \gcd(a, n) = 1\},$$

is the set of integers between 0 and n that are relatively prime to n.

Example. Let $n = 6$. Then $U(n) = \{1, 5\}$, and is a group under multiplication mod 6 with Cayley table

$U(6)$	1	5
1	1	5
5	5	1

Summary. In general, $U(n)$ under multiplication mod n is a group, but in order to be a group each element must have a unique inverse.

Proposition 1. Let $n \geq 2$ be a positive integer. An element $a \in \{0, 1, \ldots, n-1\}$ has a unique multiplicative inverse in $\{0, 1, \ldots, n-1\}$ under multiplication mod n iff $\gcd(a, n) = 1$.

In order to prove this, we need the following two facts:

Fact 1 (Extended Euclid's Lemma). For all positive integers a, b, c, if $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

Fact 2 (GCD as integer linear combination). For all nonzero integers a, n, there exist integers s, t such that

$$\gcd(a, n) = as + nt,$$

and $\gcd(a, n)$ is the smallest positive such integer linear combination.

Proof of Prop. 2.
($\Rightarrow$) Let $a \in \{0, 1, \ldots, n-1\}$ and assume a has a unique multiplicative inverse in $\{0, 1, \ldots, n-1\}$ under multiplication mod n.
Call this inverse s; by assumption $(as) \mod n = 1$.
Neither a nor s can be 0; otherwise $(as) \mod n$ would be 0.
By definition of mod in terms of the remainder of the division algorithm,

$$\begin{aligned} as &= qn + 1 \qquad \text{for some } q \in \mathbb{Z}, \text{ or} \\ as - qn &= 1\,. \end{aligned}$$

There can be no smaller positive integer linear combination, and so $\gcd(a, n) = 1$.

($\Leftarrow$) Let $a \in \{0, 1, \ldots, n-1\}$ and suppose $\gcd(a, n) = 1$.
By Fact 2,

$$\begin{aligned} 1 &= as + nt \qquad \text{for some } s, t \in \mathbb{Z}, \text{ or} \\ as &= -tn + 1\,. \end{aligned}$$

By definition of mod n from the division algorithm, $(as) \mod n = 1$.
We assume $s \in \{0, 1, \ldots, n-1\}$ by replacing s by $s \mod n$ if necessary, since

$$(as) \mod n = (a(s \mod n)) \mod n.$$

Now suppose a has another inverse s'. That is, suppose $(as') \mod n = 1$ for some $s' \neq s$.
Then

$$\begin{aligned} as' &= -t'n + 1 && \text{by definition of mod } n\text{, so that} \\ as + nt &= as' + nt' && \text{which factors as} \\ a(s - s') &= n(t' - t). \end{aligned}$$

Since the last line gives $n|a(s - s')$, but $\gcd(a, n) = 1$, then by Fact 1, $n|(s - s')$.
Therefore $s' \notin \{0, 1, \ldots, n-1\}$ unless $s' = s$.
Therefore a has a unique inverse s in $\{0, 1, \ldots, n-1\}$. □

Other steps to prove $U(n)$ is a group:

1. Closure: For all $a, b \in U(n)$, $\gcd(a, n) = 1$ and $\gcd(b, n) = 1 \Rightarrow \gcd(ab \mod n, n) = 1$.
2. Associativity: for “free”
3. Identity: try 1
4. Inverses: just proved above