Math 302: Abstract Algebra
Proof that $U(n)$ is a group.

Let $U(n) = \{m \in \mathbb{Z} \mid 1 \leq m < n \text{ and } \gcd(m,n) = 1\}$. Define $a \cdot b = ab \bmod n$.

Claim: $U(n)$ is a group. .

Closure: We must check that if $a, b \in U(n)$, then $ab \mod n \in U(n)$, i.e. that $1 \leq ab \bmod n < n$ and $\gcd(ab \bmod n, n) = 1$.

Suppose that $ab = np + r$ for some p and $0 \leq r < n$. Then $ab \bmod n = r$.

From a homework problems we know that $\gcd(a,n) = 1$ and $\gcd(b,n) = 1$ implies that $\gcd(ab,n) = 1$. This implies that there are integers s, t such that $abs + nt = 1$. By substitution, we can write $(np + r)s + nt = 1$, which we rearrange to give $r(s) + n(ps + t) = 1$. Since we have written 1 as a linear combination of r and n and since 1 is the smallest integer, we conclude that $\gcd(ab \bmod n, n) = 1$. Second, from the definition of modular multiplication, we know that $0 \leq ab \bmod n < n$. However, since $\gcd(ab \bmod n, n) = 1$, it must be the case that $1 \leq ab \bmod n < n$. Therefore $ab \bmod n \in U(n)$.

Associativity : Since multiplication is associative, so is modular multiplication.

Identity: It's always the case that $\gcd(1,n) = 1$, so $1 \in U(n)$ for all n. Since the product of 1 and x is x for all x, 1 is the identity in $U(n)$.

Inverses: We must check that for every element $b \in U(n)$, there is some other element $b^{-1} \in U(n)$ such that $bb^{-1} \bmod n = 1$.

Recall from another homework problem that in general, for any integer a, $ax \bmod n = 1$ has a solution if and only if $\gcd(a,n) = 1$.

Let b be an element in $U(n)$. Then by the definition of $U(n)$, we know that $\gcd(b,n) = 1$. Thus by that homework problem, we know that there is some number s such that $bs \bmod n = 1$. It may or may not be the case that $1 \leq s < n$. If it is not, we can write $s = nq + r$ for some integer q and some $0 \leq r < n$. In that case $br \bmod n = b(s - nq) \bmod n = bs \bmod n = 1$. Since $b \neq 0$ and since $br \bmod n = 1$ we can conclude that $r \neq 0$ (i.e. $1 \leq r < n$). Furthermore, using the homework problem again, we see that since $rx \bmod n = 1$ has a solution (namely $x = b$), it must be the case that $\gcd(r,n) = 1$. Thus we have shown that $r \in U(n)$. Since $br \bmod n = 1$, we have that $b^{-1} = r$.