Theorem 4.34. The set $\mathbb{Z}_n$ is a group under addition mod n.

Proof. In order to show that the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ forms a group under addition mod n, we will verify the four axioms of a group.

(0) **Closure:** Let $a, b \in \mathbb{Z}_n$. By the Division Algorithm, there exists unique $q, r \in \mathbb{Z}$ such that $a + b = nq + r$, where $0 \leq r < n$. This implies that, we have $a + b \equiv r \pmod{n}$. That is, in $\mathbb{Z}_n$, $a + b = r$, which verifies that $\mathbb{Z}_n$ is closed (since $0 \leq r < n$).

(1) **Associativity:** Let $a, b, c \in \mathbb{Z}_n$. We need to show that in $\mathbb{Z}_n$, we have

$$[(a + b) \pmod{n} + c] \pmod{n} = [a + (b + c) \pmod{n}] \pmod{n}.$$

By the Division Algorithm, there exists unique $q_1, r_1 \in \mathbb{Z}$ such that $a + b = nq_1 + r_1$, where $0 \leq r_1 < n$. This implies that $a + b \equiv r_1 \pmod{n}$. Again by the Division Algorithm, there exists unique $q_2, r_2 \in \mathbb{Z}$ such that $r_1 + c = nq_2 + r_2$, where $0 \leq r_2 < n$. Then $r_1 + c \equiv r_2 \pmod{n}$, which implies that

$$[(a + b) \pmod{n} + c] \pmod{n} \equiv r_2 \pmod{n}.$$

On the other hand, by the Division Algorithm, there exists unique $q_3, r_3 \in \mathbb{Z}$ such that $b + c = nq_3 + r_3$, where $0 \leq r_3 < n$. This implies that $b + c \equiv r_3 \pmod{n}$. Once again by the Division Algorithm, there exists unique $q_4, r_4 \in \mathbb{Z}$ such that $a + r_3 = nq_4 + r_4$, where $0 \leq r_4 < 0$. This shows that $a + r_3 \equiv r_4 \pmod{n}$. The upshot is that

$$[a + (b + c) \pmod{n}] \pmod{n} \equiv r_4 \pmod{n}.$$

It remains to show that $r_2 = r_4$. From above, we know $r_1 = a + b - nq_1$ and $r_2 = r_1 + c - nq_2$, which implies

$$r_2 = a + b + c - n(q_1 + q_2).$$

Similarly, we can find

$$r_4 = a + b + c - n(q_3 + q_4).$$

It follows that

$$r_2 - r_4 = n(q_1 + q_2 - q_3 - q_4),$$

which implies that $r_2 - r_4$ is divisible by n. But by Theorem 4.32, it must be the case that $r_2 \equiv r_4 \pmod{n}$. Since $0 \leq r_2, r_4 < n$, it must be the case that $r_2 = r_4$, which proves the desired result.

(3) **Inverses:** Let $a \in \mathbb{Z}_n$. Notice that $n - a \in \mathbb{Z}_n$. Moreover, in the integers, $a + (n - a) = n$. However, n is equivalent to 0 mod n, and hence $a + (n - a) = 0$ in $\mathbb{Z}_n$. This shows that $n - a$ is the (additive) inverse of a in $\mathbb{Z}_n$.

Since Axioms 0–4 hold, we have shown that $\mathbb{Z}_n$ is a group under addition mod n. □