Remark.
Let $m$ and $n$ be positive integers. By definition, $\text{lcm}(m, n)$ is the smallest positive integer $k$ such that $m|k$ and $n|k$, i.e. it is the smallest integer of the form $m + m + \cdots + m$ which is also a multiple of $n$. Therefore, the number of times one needs to add $[m]$ to itself in order to get $[0]$ in $\mathbb{Z}_n$ is $\frac{\text{lcm}(m, n)}{m}$, which is also equal to $\frac{n}{\gcd(m, n)}$ because $mn = \gcd(m, n) \text{lcm}(m, n)$.

Definition.
The additive order of an element $r$ in a ring $R$ is the minimal positive integer $k$ such that $r + \cdots + r$ $k$-times is equal to 0. If $R$ has an identity then the multiplicative order of a unit $r$ is the minimal positive integer $k$ such that $r^k = 1$. If such $k$ does not exist, we say the order is $\infty$.

Exercise.
What is the additive order of $[22]$ in $\mathbb{Z}_{55}$?
Solution.
$\gcd(22, 55) = 11$, so the additive order of $[22]$ is $\frac{55}{11} = 5$.

Exercise.
What is the multiplicative order of $[2]$ in $\mathbb{Z}_5$?
Solution.

Exercise.
Let $n$ be a positive integer and let $[m] \in \mathbb{Z}_n^\times$. Prove that the multiplicative order of $[m]$ divides $\varphi(n)$.
Solution.
Let $k$ be the order of $[m]$. Divide $\varphi(n)$ by $k$ with remainder: $\varphi(n) = qk + r$. Then $[m]^{\varphi(n)} = [1]$, but also $[m]^{\varphi(n)} = [m]^{qk+r} = ([m]^k)^q \cdot [m]^r = [m]^r$. If $r \neq 0$, it contradicts the minimality of $k$, so $r$ must be 0.
Exercise.
Prove that if $R$ is an integral domain then the additive order of 1, if finite, must be prime.

Solution.
Assume that the order $k$ of 1 is not prime. Then $k = ab$ for some integers $k - 1 \geq a, b \geq 2$. Let $r = 1 + \cdots + 1$ $a$-times and $s = 1 + \cdots + 1$ $b$-times. Because of the minimality of $k$, $r, s \neq 0$. However, $rs = 1 + \cdots + 1$ $k$-times, so $rs = 0$, which means that $r$ and $s$ are zero divisors, contradictory to the assumption that $R$ is a field.

Definition.
The additive order of 1 in an integral domain $R$ is called the characteristic of $R$, and denoted $\text{char}(R)$. If it is $\infty$, then in many texts they prefer to define the characteristic to be 0. We shall use 0 as well.

Examples.

- For prime $p$, $\mathbb{Z}_p$ is a field and $\text{char}(\mathbb{Z}_p) = p$.
- By definition, $\mathbb{Z}_0$ is isomorphic to $\mathbb{Z}$, and $\text{char}(\mathbb{Z}) = \infty$. This gives motivation for defining the characteristic to be 0 instead of $\infty$.
- $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$.

Exercise.
Let $R$ be a field of characteristic 2 of size 4, i.e. $R = \{0, 1, a, b\}$. Find the addition table and multiplication table of $R$. 