Here I present a useful theorem (in two parts) that dates back to (at least) Euclid.

Theorem: Let $m \in \mathbb{Z}_{>0}$. Let $n \in \mathbb{Z}_{>0}$. Then there exist $k, r \in \mathbb{Z}$ with $0 \leq r < m$ such that

$$n = mk + r.$$

Proof: Let $m \in \mathbb{Z}_{>0}$.
Suppose $m = 1$. Then, for any $n \in \mathbb{Z}$, $n = n \cdot m + 0$, and $0 < m$.
Suppose $m > 1$.
We will use induction on n.
Let $P(n)$ be the statement "$\exists k, r \in \mathbb{Z}$ with $0 \leq r < m$ such that $n = km + r$".
Suppose $n = 1$. Then $n = 0 \cdot m + 1$, and $1 < m$, so $P(1)$ is true.
Suppose $P(n)$ is true for some $n = x \geq 1$.
Then $x = km + r$ with $k, r \in \mathbb{Z}$ and $0 \ \leq r < m$.
Then $x + 1 = km + (r + 1)$.
Since $r < m$, we have $r + 1 \leq m$.
If $r + 1 < m$, then we are done.
If $r + 1 = m$, then $x + 1 = km + m = (k + 1)m + 0$ and $0 < m$.
Thus, $P(x + 1)$ is true.
Hence, $P(x)$ implies $P(x + 1)$.
Since $P(1)$ is true, by induction $P(n)$ is true for all $n \geq 1$.

■

Theorem: Let $m \in \mathbb{Z}_{>0}$. Let $n \in \mathbb{Z}_{>0}$. Then the integers k and r given in the above theorem are unique.

Proof: Let $m \in \mathbb{Z}_{>0}$. Let $n \in \mathbb{Z}$.
Suppose $n = k_1m + r_1 = k_2m + r_2$, with $0 \leq r_1 < m$ and $0 \leq r_2 < m$.
Then $(k_1 - k_2)m = r_2 - r_1$.
Suppose, without loss of generality, that $r_2 > r_1$.
Then $0 \leq r_2 - r_1 < m$, and, since $m | r_2 - r_1$, $r_2 - r_1 = 0$.
So $r_2 = r_1$.
Hence, $(k_1 - k_2)m = 0$.
Since $m \neq 0$, $k_1 = k_2$.

■

Both of these theorems can be extended to negative m and negative n, but we will not need those results in this course.