The Division Algorithm

We all learned division with remainder at elementary school. Like 14 divided by 3 has reainder 2 : $14 = 3 \cdot 4 + 2$. In general we have the following

Division Algorithm. **Let** n be any integer and $d > 0$ be a positive integer. Then you can divide n by d with remainder. That is

$$n = q \cdot d + r, 0 \leq r < d$$

where q and r are uniquely determined.

Given n we determine how often d goes evenly into n. Say, if $n = 16$ and $d = 3$ then 3 goes 5 times into 16 but there is a remainder 1 : $16 = 5 \cdot 3 + 1$. This works for non-negative numbers. If $n = -16$ then in order to get a positive remainder, we have to go beyond -16 : $-16 = (-6) \cdot 3 + 2$.

Let a and b be integers. Then we say that b divides a if there is an integer c such that $a = b \cdot c$. We write $b|a$ for b divides a

Examples:
$n|0$ for every n : $0 = n \cdot 0;$ in particular $0|0$.
$1|n$ for every n : $n = 1 \cdot n$

Theorem. *Let* a, b, c *be any integers.*
(a) *If* $a|b,$ *and* $a|c$ *then* $a|b + c$
(b) If $a|b$ then $a|b \cdot c$ for any c.
(c) If $a|b$ and $b|c$ then $a|c$.
(d) If $a|b$ and $a|c$ then $a|m \cdot b + n \cdot c$ for any integers m and n.

Proof. For (a) we note that $b = a \cdot s$ and $c = a \cdot t$ therefore $b + c = a \cdot s$
$+a \cdot t = a \cdot (s + t)$. Thus $a \mid b + c$.
For (b) we note that $b = a \cdot s$ and therefore $b \cdot c = (a \cdot s) \cdot c = a \cdot (s \cdot c)$ from which we get $ab \cdot c$.
For (c) we note that $b = a \cdot s$ and $c = b \cdot t$ thus $c = (a \cdot s) \cdot t = a \cdot (s \cdot t)$ which is $a|c$
Part (d) follows from (b) and (a).

We see that $a|b$ if in the division algorithm $b = q \cdot a + r$ one has that $r = 0$
Let a and b be any integers and let $m > 0$ be a positive integer. We say that a is congruent to b modulo $m, a \equiv b (\mathrm{mod}\, m),$ or $a \equiv_m b,$ in case that

$$m|a - b$$

Clearly:

$$a \equiv_m a; \text{if } a \equiv_m b \text{ then } b \equiv_m a; \text{if } a \equiv_m b \text{ and } b \equiv_m c \text{ then } a \equiv_m c$$

Being congruent is a reflexive, symmetric and transitive relation between integers. It is what is called an equivalence relation. It partiones the integers into congruence classes: $[n]_m = \{a|$ $a \equiv_m n\}$.

$$\text{If } a = q \cdot m + r, 0 \leq r < m$$

then

$$a \equiv_m r$$

Indeed $a - r = q \cdot m$.

If according to the division algorithm one has that if $a = q_a \cdot m + r_a, b = q_b \cdot m + r_b$ then $r_a = r_b$ iff $a \equiv_m b$
The idea is that if two positive numbers, both less than m, are congruent modulo m, then they must be equal.
Now, if $r_a = r_b$ then $a - b = q_a \cdot m - q_b \cdot m = (q_a - q_b) \cdot m$, which shows that $a \equiv_m b$.
If on the other hand, $a \equiv_m b$, then $r_a \equiv r_b$ shows that two numbers, both less than m are congruent, and by the remark above, they must be equal.

Any integer a is modulo m congruent to its remainder if divided by m. Thus there are m –many congruence classes accrding to possible remainders $0, 1, \ldots, m - 1$.
For $m = 1$ we just get one class. Any number is divisible by 1, thus has remainder 0 if divided by 1. We get $[0]_1 = \mathbb{Z}$
For $m = 2$ we get two classes. Remainder 0 gives us the even numbers while remainder 1 yields the odd numbers. Thus $[0]_2 = 2\mathbb{Z}, [1]_2 = 2\mathbb{Z} + 1 = \{2n + 1 | n \in \mathbb{Z}\}$.
We get three classes modulo 3 : $[0]_3 = 3\mathbb{Z}, [1]_3 = 3\mathbb{Z} + 1, [2]_3 = 3\mathbb{Z} + 2$
The $(n - 1)$ –classes mod n are
$[0]_n = n\mathbb{Z}, [1]_n = n\mathbb{Z} + 1, [2]_n = n\mathbb{Z} + 2, \ldots, [n - 1]_n = n\mathbb{Z} + (n - 1)$