Division Algorithm:

Let a be any integer and b be an positive integer. Then there exists unique integers q and r such that

$$a = b.q + r$$

dividend ↓ | ↳ remainder
divisors ↓ ↳ quotient

where $0 \leq r < b$.

Proof:

→ Contains 2 parts

→ Prove the existence of the integers q and r

→ To prove q and r are unique

Existence proof:

Consider, a set S

$$S = \{ a - bn \mid (n \in Z) \wedge (a - bn \geq 0) \}$$

where $S \subseteq W$

Case 1:-

Suppose $a \geq 0$

Then $a = a - b.0 \in S$. So set S is nonempty.

Case: 2

$a < 0$, we know $b \in Z^+$

, $b \geq 1$.

Then $-ba \geq -a$

$\therefore a - ba \geq 0$.

Consequently $a - ba \in S$.

In both cases, S has atleast one element so, S is non-empty.

By well ordering principle, which states that for every non-empty set of positive integer has a least element.

by which we can say that S contains a least element r.

Since $r \in S$, an integer q exists such that $r = a - bq$, where $r \geq 0$.

To prove that $r < b$.

By contradiction:

Assume $r \geq b$

Then $r - b \geq 0$

we know $r = a - bq$

$r - b \Rightarrow (a - bq) - b = a - b(q+1)$

which is in the form of $a - bn$ that is ≥ 0.

So $a - b(q+1) \in S$

by which we know $r - b \in S$.

So $b > 0$, $r - b < r$.

So $r - b < r$ and is in S.

This is a contradiction to our assumption so $0 \leq r < b$.

Uniqueness proof:

To show q and r are unique.

Let q, q', r and r' be integers such that

$a = bq + r$, $0 \leq r < b$

$a = bq' + r'$, $0 \leq r' < b$

Assume $q > q'$ and $r' - r = b(q - q')$

Since $q > q'$, then $r' - r \geq 0$

But we know $r < b$, $r' < b$

So $r' - r < b$.

Suppose acc to our assumption

$q > q'$, i.e, $q - q' > 1$

Then $b(q - q') \geq b$

i.e $r' - r \geq b$, which is a contradiction to $r' - r < b$.

$\therefore q \neq q'$.

Assume

$q' > q$ and $r - r' = b(q' - q)$

Since $q' > q$, then $r' - r \geq 0$

But we know $r < b$, $r < b'$

so $r' - r < b$.

Suppose acc to our assumption,

$q' > q$, i.e $q' - q > 1$

Then $b(q' - q) \geq b$

i.e, $r - r' \geq b$, which is a contradiction to $r - r' < b$

$\therefore q' > q$

Hence

The only posibility $q = q'$ and

hence $r = r'$

The integers q and r are unique.

Although called as division algorithm, we use familiar long division method

Mod operator :

a mod b = remainder when a is divided by b.

We know $q = a \text{ div } b = \lfloor a/b \rfloor$ - (1)

$r = a \bmod b$

$= a - bq$

$= a - b \cdot \lfloor a/b \rfloor$. [substituting (1)]