

Division Theorem/Euclidean Division

Let a, b be integers, $b > 0$. Then there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < b$.

Proof:

Split the problem into proving existence and proving uniqueness.

Proof of existence of q and r :

Expressing r through the given formula: $a = qb + r$. We have: $r = a - qb$.

We also know that $r \geq 0$

Let's consider the set of all remainders in the form $a - kb \geq 0$, where $k \in \mathbb{Z}$

$S = \{a - kb, a' - k'b', a'' - k''b'', \dots\}$, where all members are non-negative numbers (because we need to have remainders greater or equal to zero $r \geq 0$).

If we can prove that this set is non-empty then we can prove that there exist remainder in the form $a - kb \geq 0$ where $b > a - kb \geq 0$.

There are such integers:

$$b > a - kb \geq 0 \implies b > 0$$

$$b > 0 \wedge b \in \mathbb{N} \implies b \geq 1$$

For example let's take $b = 1$ and $k = -|a|$, so

$$a - kb \geq 0$$

$$a + |a| \geq 0, \text{ which is true for each } a$$

Now we know that the set S has members. We also know that the members are all non-negative, so by WOP (axiom), we can conclude that the set S has a smallest element. (1)

Let's say this element is $r = a - qb$.

In order to finish the proof of existence we should prove that $r < b$

Using proof by contradiction, let's assume $r \geq b$

$$a - qb \geq b \text{ (by substituting } r)$$

$$a - qb - b \geq 0$$

$$a - b(q + 1) \geq 0$$

this looks like the form $a - bk$, where $k = q + 1$. It's also non-negative, so it must be a member of the set of remainders S .

Let's compare $r = a - bq$ and $a - b(q + 1)$

$$a - b(q + 1) < a - bq, \text{ because } b(q + 1) > bq$$

but this is contradiction to (1), so $r < b$

This concludes the proof of existence: There exist q and r such that $a = qb + r$ and $0 \leq r < b$.

Proof of uniqueness of q and r :

To prove the uniqueness we are gonna try to show that there's q' and r' , but they are equal to q and r .

Let's assume that we can represent a in two ways:

$$a = bq + r = bq' + r'$$

$$r - r' = bq' - bq$$

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

From the existence proof we know that $0 \leq r' < b$ and $0 \leq r < b$.

Representing $-r'$ using $0 \leq r' < b$, we get $0 \geq -r' > -b$

let's sum both inequalities:

$$-b < -r' \leq 0 \quad / +$$

$$0 \leq r < b$$

$-b < r - r' < b$, which means that $|r - r'| < b$

$|b(q' - q)| < b$ (move b out of the module because $b > 0$)

$b|q' - q| < b$ dividing by $b \geq 1$

$|q' - q| < 1$

this means $-1 < q' - q < 1$. Given the fact that both q' and $q \in \mathbb{N}$ the result of their subtraction should also be in \mathbb{N}

The only way for that to be possible $q' - q = 0 \equiv q' = q$, which proves the uniqueness of q and r .