

Division Algorithm

Thm (Division Algorithm): Let $d \in \mathbb{N}$. Then for any $n \in \mathbb{Z}$, there exists a unique $q \in \mathbb{Z}$ and a unique $r \in \mathbb{Z}$ such that

$$n = dq + r$$

and $0 \leq r < d$.

$$(\forall d \in \mathbb{N})(\forall n \in \mathbb{Z})(\exists! q \in \mathbb{Z})(\exists! r \in \mathbb{Z})[(n = dq + r) \wedge (0 \leq r < d)]$$

Warm-Up: Let $d = 6$, $n = 317$. Find q and r .

Here,

q	is	the	<u>quotient</u>	
r	is	the	<u>remainder</u>	
n	is	the	<u>dividend</u>	(numerator)
d	is	the	<u>divisor</u>	(denominator)

Note: $n = dq + r$ \iff $\frac{n}{d} = q + \frac{r}{d}$

$n, d \in \mathbb{Z}$ $q, r \in \mathbb{Q}$

Proof: Let $d \in \mathbb{N}$ and $n \in \mathbb{Z}$. We must prove two things:

Existence: There exist $q, r \in \mathbb{Z}$ satisfying the theorem statement.

Uniqueness: If q_1, r_1 and q_2, r_2 both satisfy the theorem, then $q_1 = q_2$ and $r_1 = r_2$.

Part 1: Existence Consider all possible solutions to

$$n = dx + y$$

where $x, y \in \mathbb{Z}$ and $y \geq 0$.

Let S be the set of all y -values in these solutions.

i.e.,
$$S = \{y \in \mathbb{Z} \mid y \geq 0 \text{ and } (\exists x \in \mathbb{Z})(y = n - dx)\}$$

Ex: $d=6, n=317$

x	$317-6x$
\vdots	\vdots
48	29
49	23
50	17
51	11
52	5
53	-1
54	-7
\vdots	\vdots

So $S = \{5, 11, 17, 23, \dots\}$

↑
The remainder is the smallest element.

We now show that S is non-empty.

Case 1: $n \geq 0$. Then taking $x = 0$, we have

$$y = n - d(0) = n \geq 0$$

so $n \in S$.

Case 2: $n < 0$. Then taking $x = n$, we have

$$y = n - d(n) = n(1-d).$$

Since $d \in \mathbb{N}$, $1-d \leq 0$. So $n(1-d) \geq 0$,
and hence $n(1-d) \in S$.

Therefore S is nonempty. By the Well-Ordering Property, S has a smallest element. Call it r .

Why does this work? If $0 \in S$, then 0 is the smallest element. Otherwise, S is a subset of \mathbb{N} and we can use Well-Ordering.

Since $r \in S$, there exists $q \in \mathbb{Z}$ such that

$$n = dq + r.$$

The only thing left to show is that $0 \leq r \leq d-1$.

Because $r \in S$, we have $0 \leq r$.

Suppose that $r > d-1$. Then $r \geq d$ (since $r \in \mathbb{Z}$),
so $r-d \geq 0$.

But since

$$n - d(q+1) = (n-dq) - d = r - d,$$

this means that $r-d \in S$. But this contradicts
the fact that r is the least element of S .

So $a \leq d-1$ must be true. ✓

Part 2: Uniqueness Suppose now that $q_1, q_2, r_1, r_2 \in \mathbb{Z}$
are such that

$$n = dq_1 + r_1,$$

$$n = dq_2 + r_2,$$

and $0 \leq r_1 \leq d-1$, $0 \leq r_2 \leq d-1$.

Now, $dq_1 + r_1 = dq_2 + r_2$,

so

$$r_1 - r_2 = dq_2 - dq_1 = d(q_2 - q_1).$$

Thus, $d \mid (r_1 - r_2)$. But $-(d-1) \leq r_2 \leq 0$, so

$$d \cdot (-1) < -(d-1) \leq \underbrace{r_1 - r_2}_{d \cdot (q_2 - q_1)} \leq d-1 < d \cdot 1$$

So the only possibility is $r_1 - r_2 = 0$, i.e., $r_1 = r_2$.

Now, $r_1 - r_2 = 0 = d \cdot (q_2 - q_1)$. Since $d \neq 0$ ($d \in \mathbb{N}$), this forces $q_2 - q_1 = 0$, i.e. $q_1 = q_2$. ✓

