Division theorem / Euclidean Division

Viktor Nonov

April 23, 2018

Let a, b be integers, $b > 0$. Then there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < b$.
In notation:
$(\forall a, b \in \mathbb{Z})(b > 0)(\exists! q, r \in \mathbb{Z})[a = bq + r \wedge 0 \leq r < b]$.

Exploration

Let's start by exploring the description a bit more and add more details about the members of the division:
Reminder is the amount left over after performing division.
Let's say you divide: $a/b = q$ (remainder r), where a can be expressed as $a = bq + r$
q is the quotient which is the integer result of the division, so $q \in \mathbb{Z}$.
r can be expressed as: $r = a - qb$, where $a, b \in \mathbb{Z}$, $b > 0$ and $q \in \mathbb{Z}$.
Also in order for r to be the remainder of divison: a/b, then r should be between 0 and b: $0 \leq r < b$
I'm going to split the proof into two different sections: proving existance and proving uniqueness.

Proof:

Split the problem into proving existance and proving uniqueness.

Proof of existance of q and r:

To prove existance of r and q, we should prove them one by one:
Let's start with r.

Proof of existance of r:

Let's start exploring by trying out some specific examples, which would help construct the general case.
For example: $a = 27$ and $b = 5$, then the reminder would be $r = 2$ and quotient $q = 5$
having the expression for r: $r = a - bq$, we need to use n (which would have similar properties) instead of q since we don't know if q exists yet: $r = a - bn$, where $n \in \mathbb{Z}$.
let's try to see what are the possible values for $r = a - bn = 27 - 5n$, when we have $n = \{... - 1, 0, 1, 2, 3, 4, 5, ...\}$:
...
$n = -1 \rightarrow r = 32$
$n = 0 \rightarrow r = 27$
$n = 1 \rightarrow r = 22$
$n = 2 \rightarrow r = 17$
$n = 3 \rightarrow r = 12$
$n = 4 \rightarrow r = 7$
$n = 5 \rightarrow r = 2$
$n = 6 \rightarrow r = -3$
...
So values for r are a progression of numbers: $\{..., -3, 2, 7, 12, 17, 22, 27, 32, ...\}$
Looking at that progression we notice the reminder for division a/b is the smallest non-negative member: $remainder = 2$.
So using this hint, we can try to prove that r exists by proving that a given set has smallest non-negative member. The

Well-ordering principle states that every non-empty set of positive integers contains a least element, which might be useful. Let's consider only the positive values in the progression above, namely: $\{2, 7, 12, 17, 22, 27, 32, ...\}$, then the least element of that set is 2, which is the reminder that we are looking for. We need to construct a set for the general case and then prove that the set is non-empty, which would mean that it has least element (by WOP), which will prove that r exists.

Let's consider the following set $S = \{a - nb | a - nb \geq 0 \land n \in \mathbb{Z}\}$ - contains only positive integers, so we need to prove that is non-empty:

Proof of $(\forall a, b \in \mathbb{Z})(b > 0)(\exists n \in \mathbb{Z})[S = \{a - nb | a - nb \geq 0\}$ is non-empty]:
Using proof by cases:
1) $a \geq 0$:
$(\forall a, b \in \mathbb{Z})(a \geq 0)(b > 0)(\exists n \in \mathbb{Z})[S = \{a - nb | a - nb \geq 0\}$ is non-empty]:
Let $n = 0$. Then a member of the set would look like this:
$a - b0 \geq 0 \Leftrightarrow a \geq 0$ for each $a \geq 0$ and b, which means that the set is non-empty.
2) $a < 0$
Adding it to the expression above: $(\forall a, b \in \mathbb{Z})(a < 0)(b > 0)(\exists n \in \mathbb{Z})[S = \{a - nb | a - nb \geq 0\}$ is non-empty]:
Let $n = a$:
A member of the set will be: $a - bn = a - ba = a(1 - b)$
$1 - b \leq 0$, because $b \in \mathbb{Z} \land b > 0$, so
$a * (1 - b) \geq 0$, since a is negative and $1 - b$ is non-positive. This shows that the set is non-empty.

By proving both cases we proved that the set S is non-empty and via the WOP it has least element.

Let's name the least element r. Given the definition of a member of the set we have: $r = a - bn_r$ (n_r gets us the least member of the set S). Now it remains to prove that $0 \leq r < b$.

Proof of $0 \leq r < b$:
$r \geq 0$ because $r \in S$.
Proof of $r < b$:
Prove by contradiction:
Assume that $r \geq b$, then substituting r we get:
$a - bn_r \geq b$
$a - bn_r - b \geq 0 \Leftrightarrow a - b(n_r + 1) \geq 0$, which means that $a - b(n_r + 1) \in S$, but at the same time $a - b(n_r + 1) < a - bn_r$, which means that $a - b(n_r + 1) < r$, but r is the smallest element in S, which is contradiction.
So $r \geq b$, which concludes the proof that $0 \leq r < b$.

After we proved that r exists, we can continue to prove that q exists.

Proof of existance of q:

From the expression $a = bq + r$, we get $q = \frac{a-r}{b}$ (1).
Since we proved that r exists and $r = a - bn_r$, we substitute r in (1):
$q = \frac{a-(a-bn_r)}{b} = \frac{bn_r}{b} = n_r$, which shows that q exists.

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 existance 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 inequalitites:
$-b < -r' \leq 0$ /+
$0 \leq r < b$

$-b < r - r' < b$, 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.