Chapter 15 – The Division Theorem

Theorem 15.1.1 (The division theorem):

Let a and b be integers with $b>0$. Then there are unique integers q and r such that

$$a = b\underset{\text{"quotient"}}{\underset{\nearrow}{q}} + \underset{\text{"remainder"}}{\underset{\uparrow}{r}} \quad \text{and} \quad 0 \leq r < b.$$

$$\boxed{\frac{a}{b} = q + \frac{r}{b}}$$

This is a very familiar fact. The formal proof is also not difficult (think of why you know this is true). It is clearly presented in the book, and we follow that presentation (there's not much room for innovation).

Proof: We first prove the existence of such numbers q and r. Consider the case where $a \geq 0$. Define the set

We want to find the largest element of this set. →

$$A = \{ k \in \mathbb{Z} \mid k \geq 0 \text{ and } bk \leq a \}.$$

Then $0 \in A$, so A is non-empty. Moreover, the set A is finite since if $k \in A$ then $k \leq bk \leq a$ (since $b \geq 1$) so $A \subseteq \{0, 1, \dots, a\}$. So A has a maximum. Take $q = \max A$, and $r = a - bq$. Then $r \geq 0$ since $q \in A$ (so $bq \leq a$). Moreover $r < b$, since if r were greater than or equal to b then $b+1$ would be in A which would contradict the fact that $b = \max A$. So $a = bq + r$ and $0 \leq r < b$.

Now consider the case where a is negative. From the above we know that there are integers q' and r' such that

$$-a = bq' + r' \quad \text{and} \quad 0 \leq r' \leq b.$$

Then $a = b(-q') - r' = b(-q'-1) + (b-r')$.

(i) If $r' = 0$, take $q = -q'$, and $r = 0$.

(ii) If $r' > 0$, take $q = -q' - 1$, and $r = b - r'$.

In either case $a = bq + r$ and $0 \leq r < b$. This proves the existence part.

To prove uniqueness suppose that q_1, r_1 and q_2, r_2 satisfy $a = bq_i + r_i$ and $0 \leq r_i < b$ for $i = 1, 2$. Suppose, without loss of generality, that the q_i's have been labelled such that $\underline{\underline{q_1 \geq q_2}}$. Then

$$0 \leq r_1 = a - bq_1 \leq r_2 = a - bq_2 < b$$

so (noting that $r_1 \leq r_2 < b$ implies $\underline{0 \leq r_2 - r_1 < b - r_1 \leq \underline{b}}$) we have

$$0 \leq (a - bq_2) - (a - bq_1) < b.$$

Hence $0 \leq b(q_1 - q_2) < b$, which gives $0 \leq \underbrace{q_1 - q_2}_{\text{integer}} < 1$, i.e. $q_1 - q_2 = 0$.

It follows that $q_1 = q_2$ and $r_1 = a - bq_1 = a - bq_2 = r_2$. This concludes the proof of uniqueness. □

Example: Find the quotient and remainder when 17 is divided by 3.

$$\longrightarrow \quad 17 = 3 \times \underline{\underline{5}} + \underline{\underline{2}}.$$

Example: Find the quotient and remainder when 4725 is divided by 37.

$\longrightarrow$ Since $\frac{4725}{37} = 127.\overline{702}$,

$$4725 = 37 \times \underline{\underline{127}} + \underline{\underline{26}}.$$

An Application:

Proposition: Let $a \in \mathbb{Z}$. Then a^2 is divisible by 3 if and only if a is divisible by 3.

Proof:

Note that the reverse implication is easy. If a is divisible by 3 then $a = 3k$ for some $k \in \mathbb{Z}$, so $a^2 = 9k^2 = 3(3k^2)$, and hence a^2 is divisible by 3 (since $3k^2 \in \mathbb{Z}$).

For the forward implication we prove the contrapositive, namely that if a is not divisible by 3 then a^2 is not divisible by 3.

Suppose a is not divisible by 3 (shorthand $\underline{3 \nmid a}$).

↑ "3 does not divide a"

Then writing $a = 3q + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < 3$ we must have $r = 1$ or $r = 2$.

Case 1 ($r=1$): If $a = 3q+1$ then

$$a^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(3q^2+2q) \underline{+1}$$

so that a^2 is not divisible by 3 (since a^2 has remainder 1 when we divide by 3).

Case 2 ($r=2$): If $a = 3q+2$ then

$$a^2 = (3q+2)^2 = 9q^2 + 12q + 4$$
$$= 3(3q^2 + 4q + 1) + 1$$

so that again a^2 is not divisible by 3.

The result follows. $\square$

<u>Exercise</u>: Prove that if $n \in \mathbb{N}$ is a perfect square (meaning the square of some integer) then $n = 3q$ or $n = 3q+1$ for some $q \in \mathbb{Z}$.

↑ (This is Proposition 15.2.3.)