Mathematics 546 Homework, August 23, 2020

We use the notation $\mathbb{Z}$ for the integers and $\mathbb{N}$ for the natural numbers. There is no universal agreement on what whither 0 is a natural number. In our text it is, so the natural numbers are the set

$$\mathbb{N} := \{0, 1, 2, 3, \ldots\}.$$

(Here the symbol := means that "equal by definition".)

I assume that your are familiar with the usual algebraic properties of the integers (commutative laws, associative laws, distributive law etc.)

Definition 1. An integer a is a ***multiple*** of the integer b if and only if there is an integer q such that $a = qb$. In this case we also say that b is a ***divisor*** of a, or that b is a ***factor*** of a.

The standard notation for "b divides a" is $b \mid a$. If b does not divide a we write $b \nmid a$.

Proposition 2. *If $a, b, c \in \mathbb{Z}$ and $a \mid b$ and $a \mid c$. Then $a \mid (b - c)$. That is if a divides both a and b, then a divides the difference $b - c$.*

Proof. By the definition of $a \mid b$ and $a \mid c$ there are integers q_1 and q_2 such that

$$b = q_1 a \qquad c = q_2 a.$$

Therefore

$$b - c = q_1 a = q_2 a = (q_1 - q_2)a = qa$$

where q is the integer $q = q_1 - q_2$. Thus $a \mid (b - c)$. □

This can be generalized.

Proposition 3. *Let $a, b, c \in \mathbb{Z}$ with $a \mid b$ and $a \mid c$. Then for any $x, y \in \mathbb{Z}$*

$$a \mid (bx + cy).$$

Problem 1. Prove this. *Hint:* The proof can be carried out very much like the proof of Proposition 2. □

Here is a slightly more complicated example.

Proposition 4. *For all $a \in Z$ show that $2a^2$ is a factor of $6a^3 - 10a^2$. In symbols this is $(2a^2) \mid (6a^3 - 10a^2)$.*

Proof. This does not really involve much more than factoring and using the definition:

$$6a^3 - 10a^2 = 2a^2(3a - 5) = q(2a - 5)$$

where q is the integer $q = 2a - 5$. Thus $(2a^2) \mid (6a^3 - 10a^2)$. □

Problem 2. This problem combines both the methods we have just used. If $a \mid b$, show that $3a^3 \mid (15b^5 + 6a^2)$. □

Axiom 5 (The Well Ordering Principle)**.** *Every non-empty subset of the natural numbers has a smalles element.* □

A somewhat more detailed statement is that if $S \subseteq \mathbb{N}$ and $S \neq \varnothing$, then there is a $s_0 \in S$ such that $s_0 \leq s$ for all $s \in S$.

Theorem 6 (Divisor Algorithm)**.** *Let $a, b \in Z$ with $b > 0$. There are are unique integers q and r such that*

$$a = qb + r \qquad \textit{with } 0 \leq r < b.$$

*(The integer q is the **quotient** and r is the **remainder**.*

Problem 3. Prove the existence of q and r by doing the following steps: Let R be the set of integers

$$R := \{a - kb : k \in \mathbb{Z}\}.$$

and let R^+ be the non-negative elements in R. That is $R^+ = \{r \in R : r \geq 0\}$.

(a) Show that R^+ is non-empty. *Hint:* One what to do this is to show that $a - kb \geq 0$ when ever $k \leq a/b$.

(b) By the Well Ordering Principe R^+ has a smallest element. Let r be this smallest element. Explain why there is an integer q so that

$$r = a - qb.$$

This this is equivalent to $a = qb + r$.

(c) We are most of the way to the end. We have $a = qb + r$ and $r \geq 0$ because $r \in R^+$. We only need show $r < b$. Towards a contradiction assume $r \geq b$ and explain why this implies

$$0 \leq r - b = a - qb - b = a - (q + 1)b < r$$

and thy this is a contradiction. □

Problem 4. We are not quite done with the proof of the division algorithm, we still have to show uniqueness. That is we have to show if

$$a = q_1 b + r_1 \qquad \text{with } 0 \leq r_1 < b$$
$$a = q_2 b + r_2 \qquad \text{with } 0 \leq r_2 < b$$

then $q_1 = q_2$ and $r_1 = r_2$. Prove this. *Hint:* we have

$$a = q_1 b + r_1 = q_2 b + r_2$$

which can rearranged as

$$(q_1 - q_2)b = r_2 - r_1.$$

Use this and that $0 \leq r_1, r_2 < b$ to show $|r_2 - r_1| < 1$. Since $r_1 - r_1$ is an integer this implies $r_2 - r_1 = 0$. □