Mathematics 546 Homework, August 28, 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 set of natural numbers is

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

(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 $3a^3 \mid (15b^5 + 6a^3)$. □

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

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

*(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

$$\begin{aligned} a &= q_1 b + r_1 && \text{with } 0 \leq r_1 < b \\ a &= q_2 b + r_2 && \text{with } 0 \leq r_2 < b \end{aligned}$$

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 $r_2 - r_1 = 0$. □

Theorem 7. *Let $I \subseteq \mathbb{Z}$ be a set of integers such that*

(i) $I \neq \varnothing$.

(ii) I is closed under addition and subtraction. That is is $x, y \in I$ than also $x + y \in I$ and $x - y \in I$.

Then either $I = \{0\}$ or there is a positive number b such that I is the set of all integral elements of b. That is

$$I = \{qb : q \in \mathbb{Z}\}.$$

Problem 5. Prove this along the following lines. First note if $I = \{0\}$, then we are done so assume that $I \neq \{0\}$. That is for the rest of the proof assume that there is at least one element $x \in I$ with $x \neq 0$.

(a) Show that $0 \in I$. *Hint:* Let $x \in I$. Then as I is closed under subtraction $x - x \in I$.
(b) Show that if $x \in I$ then for any positive integer n, that $nx \in I$. *Hint:* Use that I is closed under addition and therefore $2x = x + x \in I$, $3x = x + x + x \in I$, $4x = x + x + x + x \in I$ etc.
(c) Show that if $x \in I$ then so is nx for all integers n. *Hint:* If $n > 0$ this follows by part (b). If $n < 0$, then $-n > 0$ and so, part (b) again, $(-n)x \in I$, and $0 \in I$ (part (a)) and I is closed under subtraction and thus $0 - (-n)x \in I$.
(d) Let I^+ be the positive elements in I. Show that $I^+ \neq \varnothing$ and use the Well Ordering Principle to conclude that I^+ has a smallest element b.
(e) Let b be the smallest element of I^+ and let a be any element of I. By the division algorithm there are integers q and r so that

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

Use part (c) to show $qb \in I$ and therefore, using I is closed under subtraction, that $r \in I$.
(f) Now use that b is the smallest element of I^+ to show $r = 0$ and therefore $a = qb$.
(g) Use that a was any element of I to conclude that I is just the set of all multiples of b and thus finish the proof. □

Definition 8. Let a and b be integers, not both zero. Then a positive integers d is the ***greatest common divisor*** of a and b if and only if

(i) d is a divisor of both a and b. (In symbols $d \mid a$ and $d \mid b$), and
(ii) any divisor of both a and b is also a divisor of d. (In symbols if $c \mid a$ and $c \mid b$ then $c \mid d$.)

The greatest common divisor of a and b is denoted by $\gcd(a, b)$ or just (a, b).

Note that $\gcd(0, 0)$ is not defined. Note that every number n divides 0, and $0 = 0n$. So there and not be a greatest common divisor.

Problem 6. Let $a \in \mathbb{Z}$ with $a \neq 0$. Show

$$\gcd(a, 0) = \gcd(a, a) = |a|.$$ □

Problem 7. Let a and b be integers, not both zero. Assume that d_1 and d_2 both satisfy the defintion of being the greatest common divisor of a and b. Show $d_1 = d_2$. *Hint:* As d_1 is a divisor of both a and b and d_2 is a greatest common divisor of a and b we have that $d_1 \mid d_2$. As d_1 and d_2 are both

positive this implies $d_1 \leq d_2$. Now reverse the roles of d_1 and d_2 to show $d_2 \leq d_1$. $\square$

The last problem can be rephrased as saying that if the greatest common divisor of a and b exists, then it is unique.