Weekly Homework 2

Ruth Vanderpool
TMATH 402 Abstract Algebra I

October 18, 2022

Theorem (Division Existence). Let a and b be integers with $b > 0$. Then there exists integers q and r where $0 \leq r < b$ and

$$a = bq + r.$$

Proof. Let a and b be integers with $b > 0$. To help us find q and r such that $a = bq + r$ where $0 \leq r < b$ we will rearrange the equation to $r = a - bq$. Consider letting q vary and collecting the set of all possible 'remainders', that is, let

$$R = \{a - bk | k \in \mathbb{Z} \text{ and } a - bk \geq 0\}.$$

We will consider two cases: if $0 \in R$ and if $0 \notin R$. In both cases we will identify q and r that satisfies the above conclusions of the theorem.

Case 1: Assume $0 \in R$. Then there exists a $k \in \mathbb{Z}$ such that $0 = r = a - bk$ or $bk = a$. We can let $q = k$ and $r = 0$ and satisfy the conclusions of the theorem. In particular, note $r = 0$ satisfies $0 \leq r < b$ and also that,

$$\begin{aligned} bq + r &= bq + 0 \\ &= bk \\ &= a. \end{aligned}$$

Case 2: Assume $0 \notin R$. We would like to use the Well Ordering Principal to identify the smallest number in the set R to identify the q and r needed for this theorem. Recall the Well Ordering Principal requires us to verify that the set R is nonempty.

We will show R is nonempty using two cases (2a & 2b): if $0 \leq a$ and if $a < 0$.

Case 2a: Assume that $0 \leq a$. Notice then if we choose $k = 0$, that $0 \leq a - b \cdot 0$, so we have identified an element $(a - b \cdot 0)$ in R.

Case 2b: Assume that $a < 0$. Notice then if we choose $k = 2a$, that $a - b(2a) = a(1 - 2b)$. Recall in this case that $a < 0$ and since b was assumed to be positive in the hypothesis of the theorem, we know $(1 - 2b) < 0$. A negative times a negative is a positive, thus we know $a(1 - 2b) > 0$, implying that we have identified an element $(a - b2a)$ in R.

Now that we have shown R to be nonempty we can use the Well Ordering Principal to identify the smallest number in R. Denote the smallest number as r'. By construction of R then we know there exists an integer q' such that $r' = a - bq'$. We claim that this r' and q' will meet the conclusions stated in the theorem.

Note that q' was chosen such that $r' = a - bq'$. By adding bq' to both sides we see $a = bq' + r'$ which is what we are trying to show. Notice also, by definition of R since $r' \in R$, that $0 \leq r'$. It only remains to show that $r' < b$.

Assume towards a contradiction that $r' \geq b$. Consider the element $a - b(q' + 1)$:

$$\begin{aligned} a - b(q' + 1) &= a - bq' - b \\ &= r' - b. \end{aligned}$$

Since we were assuming that $r' > b$ we see that $r' - b > 0$ implying that the element $a - b(q' - 1)$ is in the set R. The element $a - b(q' - 1)$ is also smaller than $a - bq' = r'$. But r' was identified as the smallest element in R, thus we have a contradiction! We can thus conclude that $r' < b$ which completes the proof.

□