MAT 261 HOMEWORK 8: Due Friday, Nov. 3

For integers m and n, we say that m *divides* n (or that m is a *factor* of n) if $n = km$ for some $k \in \mathbf{Z}$.

For integers $x, y \in \mathbf{Z}$, we write

$$x \equiv y \mod m$$

if $m|(x - y)$. We have shown that this is an equivalence relation (see also Hammack, p. 182), and we let $\mathbf{Z}/m\mathbf{Z}$ denote the set of equivalence classes. (Hammack denotes it by $\mathbf{Z}_m$.) For example, if $m = 12$, we saw that

$$[5] = 5 + 12\mathbf{Z} = \{\ldots, -19, -7, 5, 17, 29, \ldots\}.$$

(1) In $\mathbf{Z}/9\mathbf{Z}$, give an explicit description of the equivalence class [4].

(2) Describe the equivalence classes when $m = 1$. Do the same for $m = 0$.

(3) (a) Suppose $m > 0$. Is $\mathbf{Z}/m\mathbf{Z}$ a subset of $\mathbf{Z}$? Why or why not? What if $m = 0$?

(b) Is $\mathbf{Z}/2\mathbf{Z} \subseteq \mathbf{Z}/4\mathbf{Z}$? Why or why not?

(4) In class (on Monday 10/30/17), we'll prove that the addition rule in $\mathbf{Z}/m\mathbf{Z}$ given by

$$[a] + [b] = [a + b]$$

is well-defined. Show that likewise the multiplication rule

$$[a][b] = [ab]$$

is well-defined.

(5) Write down the addition and multiplication tables for $\mathbf{Z}/3\mathbf{Z}$ (see p. 192 for a similar example in the book).

(6) Let p be prime. Show that if $[a][b] = [0]$ in $\mathbf{Z}/p\mathbf{Z}$, then either $[a] = [0]$ or $[b] = [0]$. (Hint: this is a famous Greek guy's lemma in disguise!) Show by an example that the conclusion does not hold if $p > 1$ is composite.