Math 4000/6000 – Homework #3

posted September 12, 2018; due at the **start of class** on September 18, 2018

> The advance of mathematics has been like the rhythm of an incoming tide: the first wave, with ever slackening speed, reaches its farthest up the sand, hesitates an instant before rushing back to mingle with the following wave, which reaches a little farther than its predecessor, recedes, mingles with its successor, and so on, till the tide turns, and all are swept back to the ocean to await the next tide. In each surge forward there is some remnant of all the tides that went before, though whatever remains may long since have lost its individuality and be no more recognizable for what it was. – E.T. Bell

Assignments are expected to be neat and stapled. **Illegible work may not be marked**. Starred problems (*) are required for those in MATH 6000 and extra credit for those in MATH 4000.

0. Do but do not turn in:
   (a) Read examples 3 and 4 on pp. 40–41 of the text.
   (b) Verify that "cross-multiplication equivalence" is an equivalence relation on $\mathbb{Q}^{\text{pre}}$.

1. Let R be any ring. We say that a nonzero element a of R is a **zero divisor** if there is a nonzero $b \in R$ with $ab = 0$ or $ba = 0$. (This is the same definition of "zero divisor" as the one on p. 38 of your textbook, but there it is stated in a somewhat confusing way.) Now do Exercise 1.4.3.

   Note: In this Exercise, you may assume R is a ring; your task is to answer whether R is commutative or not and to determine, with explanation, the units and zero-divisors in R.

2. Exercise 1.4.6. *Hint:* Look back at your notes from the first few classes, and your old HW.

3. (a) Let R be a domain. Prove that if $ab = ac$ in R, and $a \neq 0$, then $b = c$.
   (b) Let R be any ring, and let x be a unit in R (i.e., an element with a multiplicative inverse). Show that x is not a zero divisor. In other words, prove that if $xb = 0$ or $bx = 0$, where $b \in R$, then $b = 0$.

4. Exercise 1.4.10.

5. Exercise 1.4.8.

6. Exercise 1.4.11.

7. (Products and sums of elements of $\mathbb{Z}_m$)
   (a) For the positive integers $m = 1, 2, 3, 4, 5$, find the sum of all of the elements of $\mathbb{Z}_m$. Formulate a general conjecture and then prove that your guess is correct.
   (b) For the primes $p = 2, 3, 5, 7$, find the product of all of the *nonzero* elements of $\mathbb{Z}_p$. Formulate a general conjecture and then prove that your guess is correct.

   Hint: An insightful approach to (a) is to 'try' to pair each element with its additive inverse. The reason 'try' is in quotes is because sometimes an element is its own additive inverse, and so your 'pair' is really just one element — can you determine when this happens? A similar strategy will work for (b), with additive replaced by multiplicative inverses.

8. Exercise 1.4.19(a,b).

9. Let p be a prime number. Find and prove a general formula for the number of squares in $\mathbb{Z}_p$.

   Example: When $p = 5$, we compute that $\bar{0}^2 = \bar{0}$, $\bar{1}^2 = \bar{1}$, $\bar{2}^2 = \bar{4}$, $\bar{3}^2 = \bar{4}$, and $\bar{4}^2 = \bar{1}$. So there are 3 distinct squares in this case, namely $\bar{0}$, $\bar{1}$, and $\bar{4}$.

10. (*) Exercise 1.4.19(c,d)

11. (*) For each positive integer number m, let $\mathbb{U}_m$ denote the set of units in $\mathbb{Z}_m$. For example, $\mathbb{U}_5 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$, while $\mathbb{U}_9 = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$.

    Fix $x \in \mathbb{U}_m$. Let $M_x \colon \mathbb{Z}_m \to \mathbb{Z}_m$ be the map $a \mapsto xa$ (the "multiplication by x map").

    (a) Show that the restriction of M_x to $\mathbb{U}_m$ yields a map from $\mathbb{U}_m$ to $\mathbb{U}_m$.

    (b) Show that the restricted map in (a) is in fact a bijection from $\mathbb{U}_m$ to $\mathbb{U}_m$.

    (c) Deduce from (b) that $\prod_{u \in \mathbb{U}_m} (xu) = \prod_{u \in \mathbb{U}_m} u$.

    (d) Let $\phi(m)$ denote the number of elements of $\mathbb{U}_m$. Prove that $x^{\phi(m)} = 1$.

    (e) Suppose now that $m = p$ is prime. Explain how to use part (d) to derive another proof of Fermat's little theorem.