Math 4000/6000 – Homework #4

posted September 12, 2016; due at the **start of class** on September 19, 2016

> 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 $\mathbb{Q}^{\mathrm{pre}}$.

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.

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 an integral domain. Prove that if $ab = ac$ in R, and $a \neq 0$, then $b = c$.
   Hint: Look back at how you solved HW #2, problem #1.
   (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. This exercise supplies a proof of the claim, made in class, that every finite integral domain is a field.

   Let R be a finite integral domain. Let x be a nonzero element of R. We must show that x has an inverse.

   (a) Consider the function $M_x \colon R \to R$ defined by $M_x(a) = xa$. (Informally, M_x is the "multiplication by x map".) Prove that M_x is a one-to-one function.
   (b) Your result in (a) implies that M_x is also an onto function. Why?
   (c) Explain why M_x being an onto function implies that x is a unit in R.

8. (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 scare quotes is because sometimes an element is its own additive inverse, and so your 'pair' is really just one element — can you determine exactly when this happens? A similar strategy will work for (b); here you need to figure out which elements are their own multiplicative inverses.

9. Exercise 1.4.19(a,b).

10. Let p be a prime number. Find and prove a general formula for the number of distinct 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 $\bar{4}$.

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

12. (*) Exercise 1.4.21