Math 4000/6000 – Homework #4

posted September 20, 2015; due at the **start of class** on September 21, 2015

We all agree that your theory is crazy, but is it crazy enough? – Niels Bohr

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. (Not to turn in!) Read examples 3 and 4 on pp. 40–41 of the text.

1. Exercise 1.4.3. (Refer to p. 38 for the definition of a **zero divisor**.)

2. Exercise 1.4.6.

   Hint: For (a)–(c), look back at your notes from the first day of class 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. 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. Complete the verification from class that $\mathbb{Z}_m$ is a commutative ring. In other words, write down proofs of properties (1), (2), and (7) from the definition of a ring given on p. 38.

7. Exercise 1.4.11.

8. In this exercise we show 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 map $M_x \colon R \to R$ 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.

9. (Products and sums of elements of $\mathbb{Z}_m$)

   (a) For $m = 1, 2, 3, 4, 5$, 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 $p = 2, 3, 5, 7$, 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.

10. Exercise 1.4.19(a,b).

11. 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 $\bar{4}$.

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

13. (*) For each natural number m, let U_m denote the set of units in $\mathbb{Z}_m$. For example, $U_5 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$, while $U_9 = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$.

    Let $x \in U_m$. 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 U_m yields a map from U_m to U_m.

    (b) Show that the restricted map in (a) is in fact a bijection from U_m to U_m.

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

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

    (e) Suppose now that $m = p$ is prime. Explain how part (d) gives another proof of Exercise 4(a) from HW #3.