## MATH 4000/6000 – Homework #3

posted February 7, 2025; due February 14, 2024

> I wish I had a dollar for every time I spent a dollar, because then, yahoo!, I'd have all my money back.
> — Jack Handey

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

0. (UNDERSTANDING CHECKS; DO NOT TURN IN)

   (a) Write out a proof of the distributive law in $\mathbb{Z}_m$. Make sure you can justify each step from the defining properties of a ring.

   (b) Let $R$ be an integral domain. Prove the *law of cancelation* in $R$: If $ab = ac$ and $a \neq 0$, then $b = c$. (This problem should look familiar!)

   (c) Show that if $m \in \mathbb{Z}^+$, then $\mathbb{Z}_m$ is the zero ring if and only if $m = 1$.

   (d) In class, we only defined $\mathbb{Z}_m$ only for positive integers $m$. Could we define $\mathbb{Z}_m$ if $m < 0$? For example, would $\mathbb{Z}_{-3}$ make sense? (If so, is $\mathbb{Z}_{-3}$ the same as a system we already know?) What about $\mathbb{Z}_0$?

---

1. Recall the statement of *Fermat's Little Theorem*: If $p$ is a prime number, then $a^p \equiv a \pmod{p}$ for every integer $a$.

   Find an **efficient** way to compute $2^{65}$ mod 65. Deduce from Fermat's Little Theorem that 65 is <u>not</u> a prime.

2. Let $n \in \mathbb{Z}$. Prove that if the congruence $x^2 \equiv n \pmod{65}$ has an integer solution, then so does $x^2 \equiv -n \pmod{65}$.

3. Suppose $m$ and $n$ are positive integers. Prove that $3^m + 3^n + 1$ cannot be a perfect square.

   Hint: Work modulo 8.

4. Solve the following simultaneous congruences:

   (a) $x \equiv 1 \pmod{4}$ and $x \equiv 7 \mod 13$,

   (b) $x \equiv 3 \pmod{4}$, $x \equiv 4 \pmod{5}$, and $x \equiv 3 \pmod{7}$.

5. Let $R$ be any ring. Prove that:

   (a) $0 \cdot a = 0$ for all $a \in R$,

   (b) $(-1)a = -a$ for all $a \in R$,

   (c) $(-a)(-b) = ab$ for all $a, b \in R$,

   (d) the multiplicative identity $1 \in R$ is unique.

   *Hint:* Look back at your notes from the first few classes, and your old homework. Make sure that your arguments do not assume commutativity of multiplication. You may assume for this problem that $-a$ is uniquely defined: that is, for every $a \in R$, there is a unique $b \in R$ with $a + b = 0$. That value of $b$ is what we denote by $-a$.

   For the rest of this assignment, use the following definition of **zero divisor**: If $R$ is a ring, an element $x \in R$ is a **zero divisor** if (1) $x$ is nonzero and (2) there is a nonzero $y \in R$ with $xy = 0$ *or* there is a nonzero $y \in R$ with $yx = 0$.

6. If $R$ is a commutative ring and $n$ is a natural number, $M_n(R)$ denotes the collection of all $n \times n$ matrices with entries in $R$. Then $M_n(R)$ is itself a ring, with the operations of addition and multiplication given by matrix addition and matrix multiplication, carried out according to the usual rules. (You are not asked to check that that $M_n(R)$ is a ring.)

   In this problem we work in $M_2(\mathbb{Z})$, the ring of $2 \times 2$ matrices with integer entries. Show that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is . . .

   (a) a unit in $M_2(\mathbb{Z})$ if and only if $ad - bc = \pm 1$;

   (b) a zero-divisor in $M_2(\mathbb{Z})$ if and only if $ad - bc = 0$ and not all of $a, b, c, d$ are zero.

   Hint: It may be helpful to consider the product of $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with $\left[\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right]$. Keep in mind that $M_2(\mathbb{Z})$ is not commutative.

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 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.

8. Let $R$ be the set of all real-valued functions on the closed interval $[0, 1]$. Define addition and multiplication on $R$ as in calculus: If $f, g \in R$, then $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $x \in [0, 1]$.

   (a) Prove that $R$ is a commutative ring.

   (b) Is $R$ an integral domain? What are the units and zero divisors? Is every nonzero element of $R$ either a unit or a zero divisor?

9. Let $R$ be an integral domain with finitely many elements. Let $r_1, \ldots, r_n$ be a complete list of the elements of $R$ (without repetition). Let $r$ be a nonzero element of $R$.

   (a) Show that $r \cdot r_1, \ldots, r \cdot r_n$ is also a complete list of the elements of $R$.

   (b) Use (a) to show that $r$ has a multiplicative inverse in $R$. Deduce that $R$ is a field.

10. (*; 3 points) Let $R$ be the ring defined in Problem 8. Let $R'$ be the subset of $R$ consisting of **continuous** real-valued functions on $[0, 1]$. Show that $R'$ is a commutative ring.

11. (*; 7 points) Is $R'$ an integral domain? What are the units and zero divisors? Is every nonzero element of $R'$ either a unit or a zero divisor?