> 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 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: Read Examples 3 and 4 on pp. 40–41 of the text.

1. Let $m \in \mathbb{Z}^+$. Suppose we wish to find all integers x that solve the congruence $ax \equiv b \pmod{m}$, where $a, b \in \mathbb{Z}$ are given. Let $d = \gcd(a, m)$. Show:

   (a) If $d \nmid b$, then there are no integer solutions.

   (b) If $d \mid b$, then $ax \equiv b \pmod{m} \iff \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$. Moreover, $\gcd(a/d, m/d) = 1$.

   Remark: (a) and (b) were illustrated in class with specific examples. Your assignment is to do the general case.

2. Exercise 1.3.7.

3. Exercise 1.3.14.

4. Exercise 1.3.20(a,c,e,g).

5. Exercise 1.3.21(b,c,e,g). *Hint:* Look at Theorem 3.8 for parts (e), (g).

6. Exercise 1.4.6.

   Hint: Look back at your notes from the first few classes, and your old HW. Make sure that your arguments do not assume commutativity of multiplication.

7. Exercise 1.4.11.

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 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).

    (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.

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