Math 109 Fall 2016 Homework 8, due **Wednesday 11/23/2016** in HW boxes in the basement of AP&M by 3 pm

1 Reading and practice

Read Chapters 19-21. Do the end of chapter exercises as you read, and check your work against the answers in the back. These exercises are to test your understanding and they are not to be written up and handed in.

2 Exercises to submit on Wednesday 11/23

Exercises from the text

In the Problems V which begin on page 271 of the text, do #1, 2, 4, 5, 7, 12.

In these problems, find a solution which uses the language of congruence, even if there are other solutions. (For example, problem 1 can be done by induction; but there is an easier proof using congruence.)

Additional problem (write up and hand in)

1. Let $m \geq 1$ be a fixed modulus and consider congruence classes modulo m.

(a). Recall that a congruence class $[a]_m$ is called *invertible* if there exists a congruence class $[x]_m$ such that $[a]_m \times [x]_m = [1]_m$. Prove that $[a]_m$ is invertible if and only if $\gcd(a, m) = 1$. In addition, show that when $\gcd(a, m) = 1$, there is a *unique* congruence class $[x]_m$ such that $[a]_m \times [x]_m = [1]_m$. (Hint: show that such an $[x]_m$ exists if and only if the linear diophantine equation $ax + my = 1$ has a solution, then apply the theory of Section 18.)

(b). Given a congruence class $[a]_m$, an *additive inverse* for $[a]_m$ is a congruence class $[b]_m$ such that $[a]_m + [b]_m = [0]_m$. (For instance, if $m = 5$, then $[3]_5$ is an additive inverse for $[2]_5$ since $[3]_5 + [2]_5 = [5]_5 = [0]_5$.)

Show that every congruence class modulo m has a unique additive inverse.