MATH 109 WINTER 2007 HOMEWORK 7, DUE 2/23/07 IN CLASS

(All exercise and page numbers refer to Eccles.)

1. Reading and practice

Read Chapters 19 and 21 of the text, and do as many of the end of chapter exercises as possible.

2. Exercises to submit on Friday 2/16

1. In the Exercises V which begin on page 271, do #1,2,3,4,5,7.

In all of the above problems, the point of these exercises is to try to think in terms of the language of congruence to help simplify your proofs.

For example, in #1, the statement you need to prove can be interpreted as "show that $6^n + 1 \equiv 0(\mathrm{mod}\, 7)$ if and only if n is odd." Now can you simplify the expression $6^n + 1$ thinking modulo 7?

In #3, it is helpful to rewrite the decimal notation $n = a_k a_{k-1} \ldots a_2 a_1 a_0$ as the actual number $a_0 + 10a_1 + 100a_2 + \cdots + 10^{k-1}a_{k-1} + 10^k a_k$ and try to simplify this expression modulo 9.

2. Fix a positive integer m. In this exercise, you will study which elements of $\mathbb{Z}_m$ have *inverses*. Recall that we write $\mathbb{Z}_m$ for the set of congruence classes modulo m, and that there are m of these: $[0], [1], [2], \ldots, [m-1]$. Here $[a] = \{b \in \mathbb{Z} | b \equiv a \bmod m\}$. Now given $[a] \in \mathbb{Z}_m$, a congruence class $[b]$ is called the *multiplicative inverse* (or just *inverse*) of $[a]$ if $[a][b] = [1]$. If such a class $[b]$ exists then $[a]$ is called *invertible*.

2a. Show that if $\gcd(a, m) = 1$, then $[a]$ is invertible. (Hint: begin by using the hypothesis to find $x, y \in \mathbb{Z}$ for which $ax + my = 1$, which we can do by a theorem we proved several weeks ago.)

2b. Show that if $[a]$ is invertible, then $\gcd(a, m) = 1$. (Hint: If $[a]$ is invertible, show first that there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod m$. Then prove that if $\gcd(a, m) \neq 1$ then a contradiction is reached.)

2c. Find all of the invertible elements of $\mathbb{Z}_{15}$, using parts (a) and (b). Find inverses for each of the elements you wrote down, by inspection.