These homework problems are meant to expand your understanding of what goes on during class. Any you turn in will be graded and returned to you. Answers may or may not be posted on the web, depending on demand.

1. **An Expanded Chinese Remainder Theorem:** Given $x \in M_m$ and $y \in M_n$ where $\gcd(m, n) = 1$, there is a unique $z \in M_{mn}$ such that

$$z \equiv x \bmod m$$
$$z \equiv y \bmod n.$$

Prove this statement as follows:

   (a) Prove that $z = xnn^{-1} + ymm^{-1}$, where n^{-1} is the inverse of n modulo m and m^{-1} is the inverse of m modulo n, satisfies the equations.

   (b) Suppose z_1 and z_2 are two possible solutions. Show that $Z = z_1 - z_2$ satisfies

$$Z \equiv 0 \bmod m$$
$$Z \equiv 0 \bmod n.$$

   (c) From part (b), show that Z must be divisible by mn, and hence $Z \equiv 0 \bmod mn$. Show that this means that $z_1 \equiv z_2 \bmod mn$, or that $z_1 = z_2$ as elements of M_{mn}.

   (d) Can you state (and prove?) a general Chinese remainder theorem?

2. [See Homework 2, Problem 6] Recall that $\mathbf{Z}[\sqrt{-5}]$ is the set of numbers $a + b\sqrt{-5}$, where a and b are integers.

   (a) Show that $\mathbf{Z}[\sqrt{-5}]$ is a group under addition. (That is, the set is $\mathbf{Z}[\sqrt{-5}]$ and the operation is addition.)

   (b) Is $\mathbf{Z}[\sqrt{-5}]$ a group under multiplication? What if we require that one of a or b be non-zero? (Hint: find $c + d\sqrt{-5}$ so that $(1 + \sqrt{-5})(c + d\sqrt{-5}) = 1$.)

3. [Hard] This problem is a sketch of a proof that $(M_p, \times)$ is a cyclic group. (That is, there is an element $g \in M_p$ such that M_p is, as a set, simply $\{1, g, g^2, g^3, \ldots, g^{p-2}\}$. Put another way, there is an element $g \in M_p$ with $g^{p-1} = 1$ and $g^k \neq 1$ for $0 < k < p - 1$.)

   (a) Suppose m is an element of M_p. Let d be the smallest positive integer with $m^d = 1$. (This d is the *order* of the element m.) Show that $d|(p - 1)$.

   (b) Since $m^d = 1$, show that $(m^2)^d = 1$, $(m^3)^d = 1$, and so on up to $(m^{d-1})^d = 1$.

   (c) Show that part (b) allows us to factor $x^d - 1$ into

$$x^d - 1 \equiv x(x - m)(x - m^2)(x - m^3) \cdots (x - m^{d-1}) \bmod p.$$

   (Hint: what are the roots of the equation on the left-hand side? On the right-hand side? You may assume that a polynomial of degree d has at most d roots.)

(d) Show that part (c) implies that if M_p contains an element of order d, then it contains exactly $\phi(d)$ of them. Let us write N_d for the number of elements of order d. This problem means that $N_d = 0$ or $N_d = \phi(d)$.

(e) Let d_1, d_2, ..., d_k be the divisors of $p-1$. Show that both

$$N_{d_1} + N_{d_2} + \ldots + N_{d_k} = p - 1$$

and

$$\phi(d_1) + \phi(d_2) + \ldots + \phi(d_k) = p - 1$$

(f) Conclude from part (e) that $N_{p-1} = \phi(p-1)$. This means that there is an element of order $p-1$ in M_p, as desired.

4. A topic we won't go into too much depth with is the idea of a *subgroup*. This is a group within a group. The operation is inherited from the larger group, as is the identity (so the identity element must be in any subgroup). Consider the following examples:

(a) Show that the elements $G = \{0, 2, 4\}$ of the group $Z_6 = \{0, 1, 2, 3, 4, 5\}$ form a subgroup. (That is, show that G is a group.)

(b) In fact, G in part (a) is *isomorphic* to $\mathbf{Z}_3 = \{0, 1, 2\}$. That is, the elements *and the multiplication table* have the "same form" (the translation of "iso" and "morph"). Show this by writing down the multiplication tables for both G and $\mathbf{Z}_3$. (This shows that $\mathbf{Z}_3$ is a subgroup of $\mathbf{Z}_6$.)

(c) Show that $C_4 = \{1, r, r^2, r^3 \mid r^4 = 1\}$ is a subgroup of

$$D_4 = \{1, r, r^2, r^3, m, mr, mr^2, mr^3 \mid r^4 = 1, m^2 = 1, mr = r^3m\}.$$

(d) For what values of k is $\{1, mr^k\}$ a subgroup of D_4?

(e) List all other subgroups of D_4 that you can find.