Homework Assignment 2

Due Friday, February 7

1. Fix $x \in \mathbb{Z}/m\mathbb{Z}$. Recall that a *multiplicative inverse* of x is an element $y \in \mathbb{Z}/m\mathbb{Z}$ so that $xy = yx = \overline{1}$.

   (a) Show that $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$.

   (b) Suppose $\overline{a}$ has a multiplicative inverse in $\mathbb{Z}/m\mathbb{Z}$. Show that this means we can solve equations of the form $\overline{a}x = \overline{b}$ for a congruence class x.

   (c) By part (a) we know that $\overline{3}$ has a multiplicative inverse in $\mathbb{Z}/7\mathbb{Z}$. What is it? Use it to solve the equation $\overline{3}x = \overline{4}$ for x.

2. Let $*$ denote multiplication modulo 15, and consider the set $\{3, 6, 9, 12\}$. Fill in the following multiplication table.

$*$	3	6	9	12
3				
6				
9				
12				

   Use the table to prove that $(\{3, 6, 9, 12\}, *)$ is a group. What is the identity element?

3. Let S be a set, and define $\mathrm{Aut}(S) := \{f : S \to S \mid f \text{ is bijective}\}$. Define a binary operation by composition $f * g := g \circ f$. Show that $\mathrm{Aut}(S)$ is a group. We will call this the *automorphism group of* S.

4. Prove the generalized associative law for groups. Explicitly, for G a group, and $b_1, b_2, \cdots, b_k$, then the product $b_1 \times b_2 \times \cdots \times b_k$ does not depend on the the bracketing. (Hint: Use induction on k, with base cases 1, 2,and 3).

5. Compute the order of every element of $(\mathbb{Z}/7\mathbb{Z})^\times$.

6. Fix an element x of a group G and suppose $|x| = n$.

   (a) Show that x^{-1} is a power of x.

   (b) Show that the all of $1, x, x^2, \cdots, x^{n-1}$ are distinct. Conclude that $|x| \le |G|$. (We will later show that if $|G|$ is finite then $|x|$ *divides* $|G|$.)

7. Fix elements x, y of a group G, and suppose $xy = e$. Show that $yx = e$.

8. Consider the presentation of the Dihedral group $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$. Use this presentation to show that every element which is not a power of r has order 2.