Homework Assignment 2

Due: Friday, February 5

1. Let $m \in \mathbb{N}$ be a natural number. Recall that the *residue of an integer x modulo m* is the remainder r when applying the division algorithm (HW1 #8) to divide x by m. We say that integers x and y are *congruent modulo m* if they have the same residue modulo m.

   (a) Show that x and y have the same residue modulo m if and only if m divides $x - y$.

   (b) Show that congruence modulo m is an equivalence relation on $\mathbb{Z}$.

   (c) Suppose $a \equiv a' \mod m$ and $b \equiv b' \mod m$. Show that:

   $$a + b \equiv a' + b' \mod m \qquad \text{and} \qquad ab \equiv a'b' \mod m.$$

2. (a) Let p be a prime number, and let $x, y \in \mathbb{Z}/p\mathbb{Z}$ be nonzero. Show that xy is also nonzero.

   (b) On the other hand, let m be a composite number greater than 3. Show that one can always find two nonzero elements of $\mathbb{Z}/m\mathbb{Z}$ whose product is zero.

3. Fix a natural number m.

   (a) Let $x, y \in (\mathbb{Z}/m\mathbb{Z})^\times$. Show that $xy \in (\mathbb{Z}/m\mathbb{Z})^\times$.

   (b) Show that $(\mathbb{Z}/m\mathbb{Z})^\times$ is a group under multiplication modulo m.

   (c) Compute the order of each element of $(\mathbb{Z}/7\mathbb{Z})^\times$

4. 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?

5. Let A be a nonempty set, and define $S_A := \{f : A \to A \mid f \text{ is bijective}\}$. Define a binary operation by composition $f * g := f \circ g$. Show that S_A is a group. We will call this the *permutation group of A*.

6. Let $(A, *)$ and $(B, \cdot)$ be two groups. Define multiplication on the Cartesian product $A \times B$ via the following rule:

   $$(a_1, b_1)(a_2, b_2) = (a_1 * a_2, b_1 \cdot b_2).$$

   Show that this makes $A \times B$ into a group. We call this group the *direct product of A and B*.

7. Fix elements x, y of a group G.

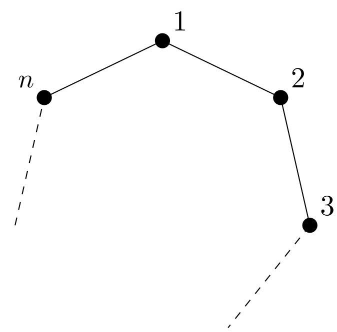
   (a) Show that if $xy = e$ then $x^{-1} = y$ and $y^{-1} = x$.

   (b) Show that $(xy)^{-1} = y^{-1}x^{-1}$.

   (c) Show that $(x^n)^{-1} = x^{-n}$.

8. Fix an element x of a group G and suppose $|x| = n$.
   (a) Show that x^{-1} is a nonnegative power of x.
   (b) Show that the all of $1, x, x^2, \cdots, x^{n-1}$ are distinct. Conclude that $|x| \leq |G|$. (We will later show that if $|G|$ is finite then $|x|$ *divides* $|G|$.)
   (c) Show that $x^i = x^j$ if and only if $i \equiv j \mod n$.

9. In class we developed the theory of the group D_{12} of rigid symmetries of the regular hexagon. In fact, everything we developed should go through almost exactly the same way for D_{2n}: the rigid symmetries of regular n-sided polygon, pictured below:



   (a) Explain why D_{2n} is a group under composition of symmetries.
   (b) Show that there are exactly $2n$ rigid symmetries of the regular n-gon.
   (c) Let r be the rotation by $2\pi/n$ in the clockwise direction, and s be the reflection along the vertical line going through the vertex labelled '1'. Compute the elements of D_{2n} in terms of r and s in the following steps:
      i. Compute the order of r and s (justifying your answers).
      ii. Let $i_1, i_2 \in \{0, 1\}$ and $j_1, j_2 \in \{0, 1, \cdots, n-1\}$. Show that:
      $$s^{i_1} r^{j_1} = s^{i_2} r^{j_2} \text{ if and only if } i_1 = i_2 \text{ and } j_1 = j_2.$$
      (Hint: You could first show $s \neq r^i$ for any i using geometry. The rest of the cases should follow from this and part (i) by using cancellation and 8(b).)
      iii. Conclude that $D_{2n} = \{s^i r^j | i = 0, 1 \text{ and } j = 0, 1, \cdots, n-1\}$. In particular, r and s generate D_{2n}.
   (d) Show that $rs = sr^{-1}$. Deduce inductively from this that $r^n s = sr^{-n}$ for all n.

We now completely understand the algebraic structure of D_{2n}. In particular, we know what every element looks like (in terms of r and s) by (c), and we know how to multiply any two elements using the relation in part (d). We summarize this by saying that D_{2n} has the following presentation:
$$D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

   (e) Use this presentation to give an algebraic proof that every element element which is not a power of r has order 2.
   (f) Bonus: Can you give a geometric interpretation of part (e)?