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 $\gcd(a, m) = 1$.

   Proof. Assume $\gcd(a, m) = 1$. Then using Euclids formula there exists x, y such that $ax + my = 1$. In particular $ax = 1 - my \equiv 1 \mod n$. In particular, $\overline{a}^{-1} = \overline{x}$.

   For the converse we first make the following observation. Let $\gcd(a, m) = g$, then for any x, y, g divides $ax + my$. This is clear as $g|ax$ since it divides a, and similarly $g|my$ so g divides their sum. Now suppose $\overline{a}^{-1} = \overline{x}$. In particular $ax \equiv 1 \mod m$ so that $ax + my = 1$ for some y. Then by our observation $g|1$, so that $g = 1$. □

   (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.

   Proof. We can multiply both sides of the equation above by $\overline{a}^{-1}$. □

   (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.

   Proof. Notice that $3 * 5 = 15 \equiv 1 \mod 7$, so that $\overline{3}^{-1} = \overline{5}$. Therefore we can multiply $\overline{3}x = \overline{4}$ by $\overline{5}$ on both sides to get $x = \overline{5} * \overline{4} = \overline{20} = \overline{6}$. Checking our work we see that $\overline{3} * \overline{6} = \overline{18} = \overline{4}$ so we are indeed correct. □

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	9	3	12	6
6	3	6	9	12
9	12	9	6	3
12	6	12	3	9

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

   Proof. Associativity follows from associativity of standard multiplication. The identity element here is 6. As 6 appears once in each column, every element has an inverse (it suffices to check columns as multiplication is commutative). □

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.

Proof. First we must show that composition on $\mathrm{Aut}(S)$ is a binary operation. Explicitly, if $f, g : S \to S$ are bijective, then so is $g \circ f$. In the first homework we showed that a function is bijective if and only if it has an inverse, so we must show $g \circ f$ has an inverse. Let f^{-1} and g^{-1} be the inverses to f and g respectively (which we know exist because they are bijective). Then:

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ id_S \circ g^{-1} = g \circ g^{-1} = id_S,$$

and

$$(f^{-1} \circ g^{-1}) \circ g \circ f = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{=1} \circ id_S \circ f = f^{-1} \circ f = id_S.$$

Therefore $g \circ f$ has inverse $f^{-1} \circ g^{-1}$ and is therefore bijective. In summary, we have show that if $f, g \in \mathrm{Aut}(S)$ then $g \circ f \in \mathrm{Aut}(S)$ so that composition is in fact a binary operation on $\mathrm{Aut}(S)$.

To show $\mathrm{Aut}(S)$ is a group we must now show that this operation (i)is associative, (ii) has an identity, and (iii) has inverses. Associativity is clear because composition of functions is associative. The identity function id_S is bijective, and for all $f \in \mathrm{Aut}(S)$ we have $id_S \circ f = f \circ id_S = f$, so the identity function serves as the identity element of the group. Finally, we showed in the first homework that f is bijective if and only if it has an inverse f^{-1}, which naturally serves as the inverse element of f in $\mathrm{Aut}(S)$. □

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

Proof. For each $a = 1, 2, \cdots, 6$ we Compute powers of a by repeatedly multiplying by a and reducing mod 7. Count how many steps it take to get to 1.

$|1| = 1$.

Powers of 2 mod 7. $2, 4, 8 \equiv 1$. So $|2| = 3$.

Powers of 3 mod 7. $3, 9 \equiv 2, 6, 18 \equiv 4, 12 \equiv 5, 15 \equiv 1$. So $|3| = 6$

Powers of 4 mod 7. $4, 16 \equiv 2, 81$. So $|4| = 3$.

Powers of 5 mod 7. $5, 25 \equiv 4, 20 \equiv 6, 30 \equiv 2, 10 \equiv 3, 15 \equiv 1$. So $|5| = 6$.

Powers of 6 mod 7, $6, 36 \equiv 1$. So $|6| = 2$. □

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

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

   Proof. Notice that x^{n-1} satisfies the property of being the inverse of x because $x * x^{n-1} = x^{n-1} * x = x^n = 1$. □

   (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* $|G|$.)

   Proof. Suppose $x^i = x^j$ for $0 \leq i \leq j < n$. Then $1 = x^{j-i}$, for $0 \leq j - i < n$. Since $x^k \neq 1$ for $0 < k < n$, we must have $j - i = 0$, so $j = i$. □

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

Proof. First multiply by $x^{-}1$ on the left to get $y = x^{-1}$. Then multiply by x on the right to get the desired result. □

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.

Proof. First notice that $r^i s = sr^{-i}$. Indeed, passing each r by s once at a time we get

$$r^i s = r^{i-1} sr^{-1} = r^{i-2} sr^{-2} = \cdots = rsr^{-(i-1)} = sr^{-i}.$$

Fix and element in D_8 which is not a power of r, then it is sr^i for some $i = 0, 1, \cdots, n-1$. Squaring we get:

$$(sr^i)^2 = sr^i * sr^i = s * s * r^{-i} * r^i = s^2 r^{i-i} = 1.$$

□