Take Home Assignment 1

Due Monday, February 24

In this assignment, we will prove an important result called *Lagrange's Theorem.* It goes as follows.

Theorem 1 (Lagrange's Theorem)**.**
If G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

With this result in hand, we will be able to deduce a celebrated result of Fermat, which is central to number theory.

Theorem 2 (Fermat's Little Theorem)**.**
Let p be a prime number and a an integer. Then $a^p \equiv a \mod p$.

To do all this, we will need the following definition.

Definition 1.
Let H be a group acting on a set A and fix $a \in A$. The orbit of a under H is the set

$$H \cdot a = \{b \in A \mid b = h \cdot a \text{ for some } h \in H\}.$$

Lets begin!

1. Let H be a group acting on a set A.
   (a) Show that the relation
   $$a \sim b \text{ if and only if } a = h \cdot b \text{ for some } h \in H$$
   is an equivalence relation on the set A.
   (b) Show that the equivalence classes of this equivalence relation are precisely the orbits of the elements of A under the action of H.
   (c) Conclude that the orbits of A under the action of H form a partition of A.

2. Let H be a subgroup of a group G, and let H act on G by left mulptilication.
   $$\begin{aligned} H \times G &\to G \\ (h, g) &\mapsto hg \end{aligned}$$
   (a) Fix $x \in G$, and consider its orbit $H \cdot x$. Show that H and $H \cdot x$ have the same cardinality. (Hint: build a bijective map $H \to H \cdot x$). Deduce that all the orbits of G under the action of H have the same cardinality.
   (b) Now suppose further that G is a finite group. Use part (a) and the exercise 1 to deduce Lagrange's theorem.

3. We can use Lagrange's theorem and what we know about cyclic groups to prove Fermat's little theorem.
   (a) Let $|G| = n < \infty$. Fix some $x \in G$. Use Lagrange's theorem to show that $x^n = 1$.
   (b) Let p be a prime number. Compute the order of $(\mathbb{Z}/p\mathbb{Z})^\times$. Fully justify your answer.
   (c) Combine parts (a) and (b) to prove Fermat's little theorem.