Math 476 - Abstract Algebra 1
Day 12 Group Assignment **Name:**______________________________

Subgroups of Cyclic Groups

Recall: Definition 22.14 A **group** G is a **cyclic group** if $G = \langle a \rangle$ for some $a \in G$.

Definition 22.17 Let G be a group and $a \in G$. If $\langle a \rangle$ is a finite group, then the element a has **finite** order. In this case, the **order** of a is equal to the order of the subgroup generated by a. If $\langle a \rangle$ is an infinite group, the element a has **infinite order**.

1. Give an example of a cyclic group of finite order and an example of a cyclic group of infinite order.

   Note: Please don't confuse the notation we use for the order of an element with absolute value. To be clear, $|a| = |\langle a \rangle|$. In words: the order of the element a is equal to the number of elements in the subgroup generated by the element a.

2. Let $G = \mathbb{Z}_8$ under the operation addition.

   (a) Find the order of each of the elements in G [see Table 23.1 on page 319 in your text].

   (b) Find the cyclic subgroups generated by $a = 2$, $a = 3$, and $a = 4$

3. Let $G = \mathbb{Z}_9$ under the operation addition.

   (a) Find the order of each of the elements in G.

   (b) Find the cyclic subgroups generated by $a = 2$, $a = 3$, and $a = 4$

4. Let $G = \mathbb{Z}_{12}$ under the operation addition.

   (a) Find the order of each of the elements in G.

   (b) Find the cyclic subgroups generated by $a = 2$, $a = 3$, and $a = 4$

Theorem 23.2 Every subgroup of a cyclic group is cyclic.

5. The goal of this Activity is to understand the proof of Theorem 23.2

   (a) State, as clearly as you can, exactly what we need to show in order to prove this theorem. [Hint: how is it quantified?]

   (b) Let H be a subgroup of G. Notice that there is one particular subgroup of G that is clearly cyclic – identify this subgroup and explain how we know it must be cyclic. If H is not that particular subgroup, what additional assumption can we make about H?

   (c) Consider any element $h \in H$. Noting that $h \in G$, how h can be expressed – what form must it have?

   (d) Given a non-trivial subgroup H of G, let $S = \{k \in \mathbb{Z}^+ : a^k \in H\}$. Explain why S must be nonempty.

   (e) What result allows us to conclude that S has a least element?

   (f) Let m be the smallest positive integer in S. That is, m is the smallest positive integer such that $a^m \in H$. Our goal is to show that $\langle a^m \rangle = H$. What must be done in order to demonstrate this?

   (g) Suppose $b \in H$. Why must $b = a^\ell$ for some integer ℓ? How does ℓ compare to m?

   (h) If we apply the division algorithm to ℓ and m, we can write $\ell = qm + r$. What can we say about r?

   (i) Since $b = a^\ell = a^{mq+r}$ and m is the smallest positive power of a that occurs in H, we must have $r = 0$. What can be conclude about b and $\langle a^m \rangle$?