Group Members: __________________________________________________________

(1) From Theorem 4.1, prove the following Corollary 1: For any group element $a$, $|a| = |\langle a \rangle|$. (Treat finite and infinite order cases separately.)

(2) From Theorem 4.1, prove the following Corollary 2: Let $G$ be a group and let $a$ be an element of order $n \in \mathbb{Z}^+$ in $G$. If $a^k = e$, then $n$ divides $k$.

Break.

**Theorem 4.2** $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.
Let $a$ be an element of order $n$ in a group and let $k$ be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$.

(3) Prove in steps the following Corollary 1 to Theorem 4.2. **Criterion for** $\langle a^i \rangle = \langle a^j \rangle$.
Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(n, i) = \gcd(n, j)$.

(a) First, use Theorem 4.2 to argue that this is equivalent to the statement that $\langle a^{\gcd(i,n)} \rangle = \langle a^{\gcd(j,n)} \rangle$ iff $\gcd(n, i) = \gcd(n, j)$.
(b) Second, figure out which direction is the easy direction and prove it.
(c) Third, use Theorem 4.2 to resolve the harder direction.
(4) Prove the following Corollary 2 of Theorem 4.2. **Generators of Cyclic Groups.**
Let \( G = \langle a \rangle \) be a cyclic group of order \( n \). Then \( G = \langle a^k \rangle \) iff gcd\( (n, k) = 1 \). (There are two directions to prove.)

(5) How does the following Corollary 3 of Theorem 4.2 follow very easily? **Generators of \( \mathbb{Z}_n \).**
An integer \( k \) in \( \mathbb{Z}_n \) is a generator of \( \mathbb{Z}_n \) iff gcd\( (n, k) = 1 \).

---

**Break.**

**Theorem 4.3 Fundamental Theorem of Cyclic Groups.**
Every subgroup of a cyclic group is cyclic. Moreover, if \( |\langle a \rangle| = n \), then the order of any subgroup of \( \langle a \rangle \) is a divisor of \( n \); and, for each positive divisor \( k \) of \( n \), the group \( \langle a \rangle \) has exactly one subgroup of order \( k \) — namely, \( \langle a^{n/k} \rangle \).