Group Members: ______________________________

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 $|a^k| = n/\gcd(n,k)$.

Corollary 1 Orders of elements in finite cyclic groups
In a finite cyclic group, the order of an element divides the order of the group.

Corollary 2 Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $|a^i| = |a^j|$
Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(n,i) = \gcd(n,j)$, and $|a^i| = |a^j|$ iff $\gcd(n,i) = \gcd(n,j)$.

Corollary 3 Generators of finite cyclic subgroups
Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ iff $\gcd(n,j) = 1$, and $|a| = |\langle a^j \rangle|$ iff $\gcd(n,j) = 1$.

Corollary 4 Generators of $\mathbb{Z}_n$
An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff $\gcd(n,k) = 1$.

---

(1) *Warmup proof.* Corollary 1 is fairly easy. Prove it in a couple of lines. Start by letting $a^k \in \langle a \rangle$ for some $k \in \mathbb{Z}$.

(2) Prove in steps Corollary 2 to Theorem 4.2.

(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.

(3) Prove Corollary 3 of Theorem 4.2. (There are two directions to prove. Use Corollary 2, and this should not be hard.)

(4) How does the following Corollary 4 of Theorem 4.2 follow very easily from Corollary 3?

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, $\langle a^{n/k}\rangle$.
