Group Activity 4C: Cyclic Groups

Group Members: ______________________________

Corollary (to FTCG) Subgroups of $\mathbb{Z}_n$.
For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k; moreover, these are the only subgroups of $\mathbb{Z}_n$.

Theorem 4.4 Number of elements of each order in a cyclic group.
If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

(1) Recall that for a positive integer d, the Euler ϕ function $\phi(d)$ is the number of positive integers k less than or equal to d and with $\gcd(d, k) = 1$. Complete the steps of the proof of Theorem 4.4.

(a) An order d element generates an order d subgroup, so what does Theorem 4.3 tell us about the number of order d subgroups?

(b) Suppose $\langle a \rangle$ is a subgroup of order d. What is the requirement for $\langle a \rangle$ to be generated by a^k where k is a positive integer?

(c) How many values k of this type are there?

(2a) For $n \geq 3$, the dihedral group D_n has order $2n$. How many elements of order n are there in D_n?

(2b) $U(21)$ is a group with order 12. In Group Activity 3B you determined that the unique cyclic subgroup of order 3 is $\{1, 4, 16\}$. How many order 3 elements are there in $U(21)$? The three cyclic subgroups of order 6 are $\{1, 2, 4, 8, 16, 11\}$, $\{1, 5, 4, 20, 16, 17\}$, and $\{1, 10, 16, 13, 4, 19\}$. How many elements of order 6 are there in $U(21)$? Express this in terms of $\phi(6)$.

Corollary (to Thm. 4.4) Number of elements of order d in a finite group
In a finite group, the number of elements of order d is divisible by $\phi(d)$.

Proof idea: Let G be a finite group, and let $a, b \in G$ both have order d. There are only two possibilities:
Case 1. $\langle a \rangle \cap \langle b \rangle$ contains no order d elements;
Case 2. $\langle a \rangle = \langle b \rangle$.

(3) Find an example of Case 1 in problem (2). Find an example of Case 2 in problem (2). Write out all the relevant subgroups or quantities.