Directions

- 1. Complete the following questions.
- 1. Suppose G is a cyclic group of order n. Show that for an integer m between 1 and n the order of g^m is $n/\gcd(m,n)$ where g is a generator.

2. Suppose G is a cyclic group of order n, show that there are exactly $\phi(n)$ generators.

3. Identify two generators of \mathbb{Z}_{13}^* .

4. \mathbb{Z}_{23}^* is a cyclic group with generator 5. Compute $DH_5(2, 20)$.

5. Prove formally that the hardness of the CDH problem relative to G implies the hardness of the discrete logarithm problem relative to G.

6. Prove formally that the hardness of the DDH problem relative to G implies the hardness of the CDH problem relative to G.