Group Members: ____

Break. Theorem 3.2 Two-Step Subgroup Test. Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H (binary operation closure), and a^{-1} is in H whenever a is in H (closure of inverses), then H is a subgroup of G.

Usage. 1. Identify the defining condition for H. 2. Prove the identity e of G fulfills this condition. 3. Assume some a, b in G fulfill the condition. 4. Prove for this a, b that ab and a^{-1} fulfill the condition.

(1) Prove that if a is an element of a group G, then the order of a is less than or equal to the order of G (Hint: get the easy case of $|G| = \infty$ out of the way first.)

Break. Theorem 3.3 Finite Subgroup Test. Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

Usage. 1. Identify the defining condition for H. 2. Prove some $a \in G$, such as e, fulfills this condition. 3. Assume some a, b in G fulfill the condition. 4. Prove for this a, b that ab fulfills the condition.

(2) Write down the elements of $U(20) = \{x \in \{1, \ldots, 19\} : \gcd(x, 20) = 1\}$, and also of $U(21) = \{x \in \{1, \ldots, 20\} : \gcd(x, 21) = 1\}$.

Definition. Let $n \geq 2$ be a positive integer, and let $2 \leq k \leq n$. Starting from the group $U(n)$ (under multiplication mod n) define the subset $U_k(n) := \{x \in U(n) : x \mod k = 1\}$.

(3) Write down the elements of the sets $U_4(20)$, $U_5(20)$, $U_3(21)$ and $U_7(21)$, by referring to (2). Which are subgroups of their parent groups?

(4) Write down the elements of the sets $U_3(10)$, $U_4(21)$, and $U_6(20)$. Which are subgroups of their parent groups?

Answer this before turning the sheet over! Which values of k make $U_k(n)$ a subgroup of $U(n)$?

(5) Prove the following using the Finite Subgroup Test: Let $n \geq 2$ be an integer, and let $k \geq 2$ be a divisor of n. Then $U_k(n)$ is a subgroup of $U(n)$.
(Hints. Non-emptiness and finiteness of $U_k(n)$ are the easy parts; closure is the key. Given $x, y \in U_k(n)$, you know four things: $\gcd(x, n) = 1$, $\gcd(y, n) = 1$, $x \mod k = 1$, and $y \mod k = 1$. Now think about closure: given $x, y \in U_k(n)$, we need $\gcd(xy, n) = 1$ and $(xy \mod n) \mod k = 1$. Use the definition of mod in terms of the division algorithm, and use the fact that $n = k \cdot d$ for some other divisor d of n.)

Break. Theorem 3.4 $\langle a \rangle$ is a Subgroup. Let G be a group, and let a be any element of G. Define $\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$. Then $\langle a \rangle$ is a subgroup of G.

---

(6) (a) Describe the cyclic subgroups of $\mathbb{Z}$ under addition. **(b)** Find all cyclic subgroups of $U(10)$ and $U(21)$.

(7) What is the largest cyclic subgroup of the dihedral group D_n (n rotations and n reflections).

Definition. The *center* of a group G is $Z(G) := \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}$. The centralizer of a fixed element a in a group G is $C(a) := \{g \in G \mid ga = ag\}$.

(8) (a) Prove that $Z(G)$ is a subgroup of G. **(b)** Prove that for a fixed element $a \in G$, that $C(a)$ is a subgroup of G.

Questions to consider. What is the relationship between Abelian-ness, $Z(G)$, and $C(a)$? Can either of $Z(G)$ and $C(a)$ be a subgroup of the other? Does it make sense to define $C(a_1, a_2)$ for distinct $a_1, a_2 \in G$?