Order

The number of elements of G is the ***order*** of G, denoted $|G|$.

The smallest positive integer n such that $a^n = e$ is the ***order*** of a, denoted $|a|$.

Order

The number of elements of G is the ***order*** of G, denoted $|G|$.

The smallest positive integer n such that $a^n = e$ is the ***order*** of a, denoted $|a|$.

Theorem. $|a| = |\langle a \rangle|$.

Order

The number of elements of G is the ***order*** of G, denoted $|G|$.

The smallest positive integer n such that $a^n = e$ is the ***order*** of a, denoted $|a|$.

Theorem. $|a| = |\langle a \rangle|$.

Theorem. $a^i = a^j$ if and only if n divides $i - j$. In particular, if $a^k = e$ then n divides k.

Cyclic groups!

The group G is ***cyclic*** if G is generated by a single element.
In other words, $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ for some $a \in G$.

Cyclic groups!

The group G is ***cyclic*** if G is generated by a single element.
In other words, $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ for some $a \in G$.

Theorems about cyclic groups.
Let a be an element of order n in a group G.

1. For a positive integer k, $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.
2. $|a^k| = n/\gcd(n,k)$.
3. In a finite cyclic group, the order of an element divides the order of the group.
4. a^k is a generator of $\langle a \rangle$ if and only if $\gcd(n,k) = 1$.
5. **(Fundamental Theorem of Cyclic Groups)**
    - Every subgroup of a cyclic group is cyclic. Specifically, every subgroup of $\langle a \rangle$ has the form $\langle a^k \rangle$ for some positive integer k.
    - For every positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k, namely $\langle a^{n/k} \rangle$.