Major Facts about Cyclic Groups

Theorem 1. **(Criterion for $a^i = a^j$)** Let G be a group and $a \in G$.

a. **If** $|a| = \infty$, **then** all distinct powers of a are distinct group elements of G;

b. **If** $|a| = n$, **then** $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ **and** $a^i = a^j$ **if and only if** $n \mid (i - j)$.

Corollary 1.1. For any $a \in G$, $|a| = |\langle a \rangle|$.

Corollary 1.2. Let $a \in G$ such that $|a| = n$. **If** $a^k = e$ for some k, **then** $n \mid k$.

Theorem 2. Let $a \in G$ such that $|a| = n$ and let $k > 0$.
Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ **and** $|a^k| = n / \gcd(n, k)$.

Corollary 2.1. **(Criterion for $\langle a^i \rangle = \langle a^j \rangle$)** Let $|a| = n$.
Then $\langle a^i \rangle = \langle a^j \rangle$ **if and only if** $\gcd(n, i) = \gcd(n, j)$.

Corollary 2.2. **(Generators of Cyclic Groups)** Let $G = \langle a \rangle$ be a cyclic group of order n.
Then $G = \langle a^k \rangle$ **if and only if** $\gcd(n, k) = 1$.

Corollary 2.3. **(Generators of $\mathbb{Z}_n$)** k is a generator of $\mathbb{Z}_n$ **if and only if** $\gcd(n, k) = 1$.

Theorem 3. **(Fundamental Theorem of Cyclic Groups)** Let $G = \langle a \rangle$ be a cyclic group.
Then

a. Every subgroup of G is cyclic;

b. **If** $|G| = n$, **then** the order of any subgroup of G divides n;

c. For each positive divisor k of n, the group G has **exactly one** subgroup of order k, that is, $\langle a^{n/k} \rangle$.

Corollary 3.1. **(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 $\mathbb{Z}_n$.