Theorem 4.1 Let G be a group, and let a belong to G. If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order, say n, then $\langle a \rangle = \{e, a, a^2, ..., a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$.

Corollary 1 For any group element a, $|a| = |\langle a \rangle|$.

Corollary 2 Let G be a group and let a be an element of order n in G. If $a^k = e$, then n divides k.

Theorem 4.2 Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{gcd(n,k)} \rangle$ and $|a^k| = \frac{n}{gcd(n,k)}$

Corollary 1 In a finite cyclic group, the order of an element divides the order of the group.

Corollary 2 Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $gcd(n, i) = gcd(n, j)$ and $|a^i| = |a^j|$ if and only if $gcd(n, i) = gcd(n, j)$.

Corollary 3 Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $gcd(n, j) = 1$ and $|a| = |a^j|$ if and only if $gcd(n, j) = 1$.

Corollary 4 An integer k in Z_n is a generator of Z_n if and only if $gcd(n, k) = 1$.

Theorem 4.3 The Fundamental Theorem of Cyclic Groups Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k, namely, $\langle a^{n/k} \rangle$.

Corollary For each positive divisor k of n, then set $\langle n/k \rangle$ is the unique subgroup of Z_n of order k; moreover, these are the ONLY subgroups of Z_n.

The Euler-Phi Function, $\phi(n)$. $\phi(n)$ denotes the number of positive integers less than n that are relatively prime to n. If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where the p_i are distinct primes and the e_i are positive integers, then $\phi(n) = (p_1^{e_1} - p_1^{e_1 - 1})(p_2^{e_2} - p_2^{e_2 - 1}) \cdots (p_k^{e_k} - p_k^{e_k - 1})$.

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

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