Cyclicity

Theorem: Let G be a finite group. Then the following conditions are equivalent:

1. G is cyclic.
2. For each $d \in \mathbf{Z}^+$, the number of $g \in G$ such that $g^d = e$ is less than or equal to d.
3. For each $d \in \mathbf{Z}^+$, G has at most one subgroup of order d.
4. For each $d \in \mathbf{Z}^+$, G has at most $\phi(d)$ elements of order d.

Proof: Suppose that G is cyclic of order n. If $d \in \mathbf{Z}^+$, let $d' := gcd(d, n)$ and write $d = d'c$ and $n = d'm$. Clearly if $g^{d'} = e$, then also $g^d = e$. Moreover, since there exist integers x, y such that $d' = xd + yn$ and $g^n = e$, $g^{d'} = g^{xd}$ so $g^d = e$ implies also that $g^{d'} = e$. Thus $g^d = e$ iff $g^{d'} = e$. Now if g_0 generates g, the set of all such g is just the subgroup of G generated by g_0^m, which has d elements. Thus (1) implies (2).

Suppose that (2) holds and $d \in \mathbf{Z}^+$. Let H be a subgroup of G of order d. Then $g^d = e$ for every $g \in G$. According to (2), there are at most d such elements. But then $H = \{g \in G : g^d = e\}$, and hence H is unique.

Suppose (3) holds. If there are no elements of order d, then there is nothing to check. If g is an element of order d, then $\langle g \rangle$ is a subgroup of order d, and by (3), it is the unique such subgroup. Hence if g' is any element of order d, $g' \in \langle g \rangle$. Since $\langle g \rangle$ contains exactly $\phi(d)$ elements of order d, we see that G has exactly $\phi(d)$ elements of order d.

Suppose that (4) holds. For each divisor d of the order of G, let $m(d)$ denote the number of elements of G of order d. Looking at the partition of the group G obtained by grouping together elements of the same order, we see that the sum of all $m(d)$ is equal to the order of G. For example, if $G = \mathbf{Z}_n$, $m(d) = \phi(d)$ if $d|n$ and $m(d) = 0$ otherwise. Thus $\sum_{d|n} \phi(d) = n$. If G is a group of order n and satisfies (3) we find that

$$n = \sum_{d|n} m(d) \leq \sum_{d|n} \phi(d) = n$$

Since each $0 \leq m(d) \leq \phi(d)$ for each d, we see that the equality $\sum_{d|n} m(d) = \sum_{d|n} \phi(d)$ implies that each $m(d) = \phi(d)$ for every d. In particular $m(n) = \phi(n) \neq 0$. This means that G has at least one elmeent of order n, and hence is cyclic. $\square$