Cyclic Group Supplement 2

Lemma 1. *A cyclic group contains at most one element of order 2.*

Put another way, an involution[1] of a cyclic group, if it exists, is unique.

Proof. Let $G = \langle a \rangle$ be a cyclic group.

If G is infinite, then there are no elements of order 2. So, assume the order of G is finite: $|G| = n < \infty$. If $n = 1$, then $G = \langle e \rangle$; if $n = 2$, then $G = \{e, a\}$ and $a^2 = e$. In both cases, there is nothing to prove.

Suppose $n > 2$, and let $x, y \in G$ be two non-identity elements of G, say, $x = a^j$ and $y = a^k$, where $1 < j, k < n$. If $x^2 = e$, then $a^{2j} = e$. Therefore n divides $2j$ (by Theorem 4(a) of Cyclic Group Supplement 1). But $j < n$ implies $2j < 2n$, so the only way to have $n|2j$ is $n = 2j$. If $y^2 = e$, then the same argument applied to k yields $n = 2k$. It follows that if $x^2 = e = y^2$, then $j = k$ and so $x = a^j = a^k = y$. Hence involutions of cyclic groups are unique. $\square$

[1] Recall, an *involution* is an element of order 2.