4.11 Theorem. Let $a, n \in \mathbb{N}$ with $n > 1$ and $(a, n) = 1$. Then $\text{ord}_n(a) < n$.

Proof. Let $k = \text{ord}_n(a)$. By Theorem 4.8, we know that the numbers of the set $A = \{a^1, a^2, ..., a^k\}$ are pairwise incongruent modulo n. Consider the set $S = \{a^1, a^2, ..., a^n\}$ as a subset of A. S has n elements and are pairwise incongruent mod n. Therefore, by Theorem 3.17, S is CRS modulo n. In particular, there exists $i \in \mathbb{N}$ with $1 \leq i \leq n$ such that $a^i \equiv 0 \pmod{n}$. By Theorem 4.2, $(a^i, n) = 1$, but by Theorem 4.3, this implies $(0, n) = 1$. However, $(0, n) = n > 1$ which contradicts the original assumption that $n > 1$. Thus, $\text{ord}_n(a) < n$. $\square$