4.8 Theorem. Let $a, n \in \mathbb{N}$ with $(a, n) = 1$ and let $k = \mathrm{ord}_n(a)$. Then the numbers $a^1, a^2, ..., a^k$ are pairwise incongruent modulo n.

Proof. Suppose not. That is, there exists a pair of numbers $1 \leq i, j \leq k$, and WLOG $i > j$, such that a^i is congruent to a^j. Let $a^i \equiv a^j \pmod{n}$. Factoring a^j, $a^{i-j}a^j \equiv a^j \pmod{n}$. By CPI, let $i - j = k' \in \mathbb{Z}$ such that $a^{k'}a^j \equiv a^j \pmod{n}$. Since $(a^j, n) = 1$, $a^{k'} \equiv 1 \pmod{n}$. Since $i, j < k$, $i - j = k' < k$. This contradicts the initial assumption that $k = \mathrm{ord}_n(a)$. Thus, the numbers $a^1, a^2, ..., a^k$ are pairwise incongruent modulo n, provided $(a, n) = 1$ and $k = \mathrm{ord}_n(a)$. $\square$