4.4 Theorem. Let $a, n \in \mathbb{N}$. Then there exist natural numbers i and j, with $i \neq j$, such that $a^i \equiv a^j \pmod{n}$.

Proof. Let $S = \{a, a^2, ..., a^n, a^{n+1}\}$ and define $t_i \in \{0, 1, ..., n-1\}$ by congruence $a^i \equiv t_i \pmod{n}$ by Theorem 3.14. Let $T = \{t_1, t_2, ..., t_{n+1}\}$ be a subset of $\{0, 1, ..., n-1\}$. T has at most n elements, and so there are $1 \leq i, j \leq n+1$ and $i \neq j$ such that $t_i \neq t_j$. Thus,

$$a^i \equiv t_j \pmod{n}.$$

Thus, $a^i \equiv a^j \pmod{n}$. $\square$