4.31 Theorem. Let n be a natural number and let $x_1, x_2, ...x_{\phi(n)}$ be the distinct natural numbers less than or equal to n that are relatively prime to n. Let a be a non-zero integer relatively prime to n and let i and j be different natural numbers less than or equal to $\phi(n)$. Then $ax_i \not\equiv ax_j \pmod{n}$.

Proof. Suppose not. That is, suppose $ax_i \equiv ax_j \pmod{n}$. Since $(a, n) = 1$, by Theorem 1.45, $x_i \equiv x_j \pmod{n}$. Let $X = \{x_1, x_2, ...x_{\phi(n)}\}$ be a subset of the CCRS modulo n. By Theorem 3.17, no two elements of X are congruent modulo n, which contradicts $x_i \equiv x_j \pmod{n}$. Thus, $ax_i \not\equiv ax_j \pmod{n}$. □