4.32 Theorem. (Euler's Theorem) If a and n are integers with $n > 0$ and $(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. Let $X = \{x_1, x_2, ..., x_{\phi(n)}\}$ be a subset of CCRS modulo n. Since $(a, n) = 1$ and $(x_i, n) = 1$ for any $1 \leq i \leq \phi(n)$, by Theorem 1.43, $(ax_i, n) = 1$. By Theorem 4.31, we know that $ax_i \not\equiv ax_j \pmod{n}$. Since the set $0, 1, ..., n-1$ is CCRS, $ax_i \equiv r_i \pmod{n}$ for some $0 \leq r_i \leq n-1$. By Theorem 4.29, $(r_i, n) = 1$. This means $r_i \in \mathbb{X}$. So it follows that each ax_i is congruent to a distinct x_j; that is, $ax_i \equiv x_j \pmod{n}$ for some $1 \leq j \leq \phi(n)$ and $i \neq j$. Thus,

$$ax_1 ax_2 ... ax_{\phi(n)} \equiv x_1 x_2 ... x_{\phi(n)} \pmod{n}.$$

Let $x' = x_1 x_2 ... x_{\phi(n)}$ and we find that

$$a^{\phi(n)} x' \equiv x' \pmod{n}.$$

Since $(x_i, n) = 1$, by Theorem 1.43, $(x', n) = 1$. Thus, by Theorem 1.45, $a^{\phi(n)} \equiv 1 \pmod{n}$. $\square$