4.10 Theorem. Let $a, n \in \mathbb{N}$ with $(a, n) = 1$ and let $k = \text{ord}_n(a)$, and let $m \in \mathbb{N}$. Then $a^m \equiv 1 \pmod{n}$ if and only if $k|m$.

Proof. Suppose $k|m$. By definition, $m = kt$ for $t \in \mathbb{Z}$. Since $k = \text{ord}_n(a)$,

$$\begin{aligned} a^k &\equiv 1 \pmod{n}, \\ (a^k)^t &\equiv 1^t \pmod{n}, \\ a^{kt} &\equiv 1 \pmod{n}. \end{aligned}$$

Thus, $a^m \equiv 1 \pmod{n}$. Now suppose $a^m \equiv 1 \pmod{n}$. Applying TDA, $m = kq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r \leq m - 1$. Since $k = \text{ord}_n(a)$,

$$\begin{aligned} a^k &\equiv 1 \pmod{n}, \\ (a^k)^q &\equiv 1^q \pmod{n}, \\ a^{kq} &\equiv 1 \pmod{n} \\ a^{kq}a^r &\equiv a^r \pmod{n} \\ a^{kq+r} &\equiv a^r \pmod{n} \\ a^m &\equiv a^r \pmod{n}. \end{aligned}$$

Since we have defined $0 \leq r \leq k - 1$, if $r \geq 1$, then $a^r \equiv 1 \pmod{n}$ contradicts $k = \text{ord}_n(a)$. Thus, $r = 0$ such that $a^m \equiv a^r \equiv a^0 \equiv 1 \pmod{n}$. This implies that $m = kq$, and by definition, $k|m$. Thus, $a^m \equiv 1 \pmod{n}$ if and only if $k|m$, provided $(a, n) = 1$ and $k = \text{ord}_n(a)$. $\square$