4.9 Theorem. Let $a, n \in \mathbb{N}$ with $(a, n) = 1$ and let $k = \text{ord}_n(a)$. For any natural number m, a^m is congruent modulo n to one of the numbers $a^1, a^2, ..., a^k$.

Proof. By TDA, let $m - qk + r$ where $0 \leq r \leq k - 1$. Since $k = \text{ord}_n(a)$, $a^k \equiv 1 \pmod{n}$. By Theorem 1.18,

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

Recall $0 \leq r \leq k - 1$. If $r = 0$, $a^m \equiv a^0 \pmod{n}$ which is $a^m \equiv 1 \pmod{n}$ and we find $a^m \equiv a^k \pmod{n}$. Thus, for any natural number m, a^m is congruent modulo n to one of the numbers $a^1, a^2, ..., a^k$. $\square$