4.18 Theorem. Let p be a prime and a be an integer. If $(a, p) = 1$, then $\mathrm{ord}_p(a)$ divides $p - 1$.

Proof. By Theorem 4.15, $a^{p-1} \equiv 1 \pmod{p}$. Since $(a, p) = 1$, by Theorem 4.10, $k|p - 1$. Thus, $\mathrm{ord}_p(a)$ divides $p - 1$. □