

6.12 Puisque p ne divise pas a , on a $\text{pgcd}(a, p) = 1$.
Le théorème d'Euler donne : $a^{p-1} \equiv a^{\varphi(p)} \equiv 1 \pmod{p}$.