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

Théorie des nombres : théorème d'Euler Corrigé 6.12