6.2 Montrons par récurrence que $\operatorname{pgcd}(a^n, m) = 1$ pour tout $n \in \mathbb{N}$.

L'hypothèse $\operatorname{pgcd}(a,m)=1$ donne l'initialisation.

Supposons que $\operatorname{pgcd}(a^n,m)=1$. Comme $\operatorname{pgcd}(a,m)=1$, on conclut, grâce à l'exercice 6.1, que $\operatorname{pgcd}(a^{n+1},m)=1$.

Théorie des nombres : théorème d'Euler Corrigé 6.2