6.5 1) Supposons qu'il existe $k \in \mathbb{N}$ avec $1 \leqslant k < m$ tel que $a^k \equiv 1 \mod m$.
L'équation $a\,x \equiv 1 \mod m$ admet a^{k-1} comme solution.
Vu la proposition de la page 4.1, a et m sont premiers entre eux.

2) Supposons a et m premiers entre eux.

(a) Clairement $\text{pgcd}(1, m) = 1$.
Par hypothèse, $\text{pgcd}(a, m) = 1$.
L'exercice 6.2 certifie que $\text{pgcd}(a^n, m) = 1$ pour tout $n \in \mathbb{N}$.
Ainsi, $\overline{a^n}$ est une unité de $\mathbb{Z}/m\mathbb{Z}$ pour tout $n \geqslant 0$.

(b) $\mathbb{Z}/m\mathbb{Z}$ ne peut avoir au plus que $m - 1$ unités.
En effet, $\mathbb{Z}/m\mathbb{Z}$ contient m classes de congruence et $\overline{0}$ n'est pas une unité.

(c) Puisqu'il ne peut y avoir plus de $m - 1$ unités, parmi les m unités $\overline{1}$, $\overline{a}$, $\overline{a^2}$, $\overline{a^3}$, ..., $\overline{a^{m-1}}$, il y en a deux d'entre elles qui sont égales.
C'est pourquoi, il existe $n \geqslant 0$ et $1 \leqslant k \leqslant m - 1$ tels que $\overline{a^{n+k}} = \overline{a^n}$, c'est-à-dire $a^{n+k} \equiv a^n \mod m$.

(d) Attendu que $\text{pgcd}(a^n, m) = 1$, l'exercice 4.2 permet de simplifier la congruence $a^{n+k} \equiv a^n \mod m$, pour obtenir $a^k \equiv 1 \mod m$.