4.7 1) En remplaçant a par $a\,x$, b par 1 et k par y dans l'énoncé de l'exercice 2.6, on obtient aussitôt : $a\,x \equiv 1 \mod m$ si et seulement s'il existe $y \in \mathbb{Z}$ tel que $1 = a\,x + m\,y$.

2) (a) Supposons que l'équation $a\,x \equiv 1 \mod m$ admette une solution.
Il existe alors des entiers x et y tels que $a\,x + m\,y = 1$.
D'après le théorème de Bachet de Mériziac, $a\,x + m\,y = k \cdot \mathrm{pgcd}(a, m)$ pour un certain entier k.
Ainsi $\mathrm{pgcd}(a, m)$ divise $a\,x + m\,y = 1$, de sorte que $\mathrm{pgcd}(a, m) = 1$: en d'autres termes, a et m sont premiers entre eux.

(b) Supposons que a et m soient premiers entre eux.
D'après le théorème de Bézout, il existe des entiers x et y tels que $a\,x + m\,y = \mathrm{pgcd}(a, m) = 1$.
Cette égalité entraîne $a\,x \equiv 1 \mod m$.