6.1 1) Vu le théorème de Bézout, il existe des entiers u, v, $u^\star$ et $v^\star$ tels que

$$a\,u + m\,v = 1 \quad \text{et} \quad b\,u^\star + m\,v^\star = 1$$

En multipliant ces deux équations, on obtient :

$1 = (a\,u + m\,v)\,(b\,u^\star + m\,v^\star) = (a\,b)\,(u\,u^\star) + m\,(a\,u\,v^\star + b\,u^\star\,v + m\,v\,v^\star)$

D'après le théorème de Bachet de Mériziac, $1 = k \cdot \text{pgcd}(ab, m)$, d'où l'on tire que $\text{pgcd}(a\,b, m) = 1$.

2) Vu la proposition de la page 4.1, il existe $x_1 \in \mathbb{Z}$ tel que $a\,x_1 \equiv 1 \mod m$ et $x_2 \in \mathbb{Z}$ tel que $b\,x_2 \equiv 1 \mod m$.

On en déduit que $(a\,b)\,(x_1\,x_2) \equiv (a\,x_1)\,(b\,x_2) \equiv 1 \cdot 1 \equiv 1 \mod m$.
Ainsi, l'équation $(a\,b)\,x \equiv 1 \mod m$ admet pour solution $x_1\,x_2$.

La proposition de la page 4.1 implique que $a\,b$ et m sont premiers entre eux, c'est-à-dire $\text{pgcd}(a\,b, m) = 1$.