

4.8 Si a et m sont premiers entre eux, alors l'équation $ax \equiv 1 \pmod{m}$ admet une solution x_0 , d'après l'exercice 4.7.

Pour tout $b \in \mathbb{Z}$, la congruence $ax_0 \equiv 1 \pmod{m}$ implique $abx_0 \equiv b \pmod{m}$, au vu de l'exercice 4.1 1).

L'équation $ax \equiv b \pmod{m}$ admet ainsi bx_0 comme solution.