2.10 1) Choisissons $a = 0$, $b = 2$ et $m = 4$.

On constate alors que

(a) $2\,a \equiv 2\,b \mod m$

(b) $a \not\equiv b \mod m$

Il est faux de conclure que $2\,a \equiv 2\,b \mod m$ implique $a \equiv b \mod m$.

2) Supposons à présent m impair.

Si $2\,a \equiv 2\,b \mod m$, alors $m \mid (2\,a - 2\,b)$, c'est-à-dire $m \mid 2\,(a - b)$.

Il existe donc $q \in \mathbb{Z}$ tel que $m\,q = 2\,(a - b)$.

Ainsi $2 \mid m\,q$.

Mais, comme m est impair, cela signifie que $2 \mid q$; en particulier $\frac{q}{2} \in \mathbb{Z}$.

En résumé, $m\,q = 2\,(a - b)$ implique $m\,\frac{q}{2} = a - b$ avec $\frac{q}{2} \in \mathbb{Z}$.

En d'autres termes, $m \mid (a - b)$, d'où l'on conclut $a \equiv b \mod m$.