6.10 1) (a) L'énoncé du théorème d'Euler suppose que $\text{pgcd}(a, m) = 1$.

Puisque $\overline{r_i}$ est une unité de $\mathbb{Z}/m\mathbb{Z}$, on a que $\text{pgcd}(r_i, m) = 1$.

L'exercice 6.1 permet de conclure que $\text{pgcd}(a\, r_i, m) = 1$.
C'est pourquoi $\overline{a\, r_i}$ est une unité de $\mathbb{Z}/m\mathbb{Z}$.

(b) Puisque a est m sont premier entre eux, $\overline{a}$ est une unité de $\mathbb{Z}/m\mathbb{Z}$ et possède donc un inverse $\overline{a}^{-1}$.

L'application $f : \begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^* \\ \overline{r_i} & \longmapsto & \overline{a\, r_i} \end{array}$ est bijective, car elle admet pour fonction réciproque ${}^r\!f : \begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^* \\ \overline{r_i} & \longmapsto & \overline{a}^{-1}\, \overline{r_i} \end{array}$.

2) En multipliant tous les éléments de $(\mathbb{Z}/m\mathbb{Z})^* = \big\{\overline{r_i} : 1 \leqslant i \leqslant \varphi(m)\big\} = \big\{\overline{a\, r_i} : 1 \leqslant i \leqslant \varphi(m)\big\}$, on obtient :

$\overline{a\, r_1} \cdot \overline{a\, r_2} \cdot \overline{a\, r_3} \cdot \ldots \cdot \overline{a\, r_{\varphi(m)}} = \overline{r_1} \cdot \overline{r_2} \cdot \overline{r_3} \cdot \ldots \cdot \overline{r_n}$

$\overline{(a\, r_1)\,(a\, r_2)\,(a\, r_3)\, \ldots\, (a\, r_{\varphi(m)})} = \overline{r_1\, r_2\, r_3\, \ldots\, r_{\varphi(m)}}$

$(a\, r_1)\,(a\, r_2)\,(a\, r_3)\, \ldots\, (a\, r_{\varphi(m)}) \equiv r_1\, r_2\, r_3\, \ldots\, r_{\varphi(m)} \mod m$

$a^{\varphi(m)}\, r_1\, r_2\, r_3\, \ldots\, r_{\varphi(m)} \equiv r_1\, r_2\, r_3\, \ldots\, r_{\varphi(m)} \mod m$

Comme $\text{pgcd}(r_i, m) = 1$ pour tout $1 \leqslant i \leqslant \varphi(m)$, l'exercice 4.2 nous autorise à simplifier cette congruence par $r_1\, r_2\, r_3\, \ldots\, r_{\varphi(m)}$, ce qui donne

$$a^{\varphi(m)} \equiv 1 \mod m$$