7.4 1) $e\,d \equiv 1 \iff e\,d - 1 = k\,\varphi(n) \iff e\,d = 1 + k\,\varphi(n)$ avec $k \in \mathbb{Z}$

Puisque $e > 1$ et $d > 1$, on a $e\,d > 1$, si bien que $k\,\varphi(n) \geqslant 0$.
De $\varphi(n) \geqslant 0$, on tire que $k \geqslant 0$.

$(a^e)^d = a^{e\,d} = a^{1+k\,\varphi(n)} = a^1 \cdot a^{k\,\varphi(n)} = a \cdot \left(a^{\varphi(n)}\right)^k$

2) (a) Si $p \nmid a$ et $q \nmid a$, alors a et $n = p\,q$ sont premiers entre eux.
Le théorème d'Euler implique $a^{\varphi(n)} \equiv 1 \mod n$.

On en déduit : $(a^e)^d = a \cdot \big(\underbrace{a^{\varphi(n)}}_{\equiv 1}\big)^k \equiv a \cdot 1^k \equiv a \mod n$.

(b) i. $p \mid a \iff p \mid (a - 0) \iff a \equiv 0 \mod p$
$(a^e)^d \equiv (0^e)^d \equiv 0^d \equiv 0 \equiv a \mod p$

ii. Le petit théorème de Fermat affirme que $a^{(q-1)} \equiv 1 \mod q$.

$$(a^e)^d = a \cdot \left(a^{\varphi(n)}\right)^k = a \cdot \left(a^{(p-1)\,(q-1)}\right)^k = a \cdot \left(a^{(q-1)}\right)^{k\,(p-1)}$$
$$\equiv a \cdot (1)^{k\,(p-1)} \equiv a \cdot 1 \equiv a \mod q$$

iii. D'après l'exercice 4.4, les congruences $\begin{cases} (a^e)^d \equiv a \mod p \\ (a^e)^d \equiv a \mod q \end{cases}$
impliquent $(a^e)^d \equiv a \mod p\,q$, car $\operatorname{pgcd}(p, q) = 1$.
On conclut en rappelant que $p\,q = n$.

(c) i. $q \mid a \iff q \mid (a - 0) \iff a \equiv 0 \mod q$
$(a^e)^d \equiv (0^e)^d \equiv 0^d \equiv 0 \equiv a \mod q$

ii. Le petit théorème de Fermat affirme que $a^{(p-1)} \equiv 1 \mod p$.

$$(a^e)^d = a \cdot \left(a^{\varphi(n)}\right)^k = a \cdot \left(a^{(p-1)\,(q-1)}\right)^k = a \cdot \left(a^{(p-1)}\right)^{k\,(q-1)}$$
$$\equiv a \cdot (1)^{k\,(q-1)} \equiv a \cdot 1 \equiv a \mod p$$

iii. D'après l'exercice 4.4, les congruences $\begin{cases} (a^e)^d \equiv a \mod p \\ (a^e)^d \equiv a \mod q \end{cases}$
impliquent $(a^e)^d \equiv a \mod p\,q$, car $\operatorname{pgcd}(p, q) = 1$.
On conclut en rappelant que $p\,q = n$.

(d) $p \mid a \iff p \mid (a - 0) \iff a \equiv 0 \mod p$
$q \mid a \iff q \mid (a - 0) \iff a \equiv 0 \mod q$

D'après l'exercice 4.4, les congruences $\begin{cases} a \equiv 0 \mod p \\ a \equiv 0 \mod q \end{cases}$
impliquent $a \equiv 0 \mod p\,q$, à savoir $a \equiv 0 \mod n$.

Par conséquent, $(a^e)^d \equiv (0^e)^d \equiv 0^d \equiv 0 \equiv a \mod n$.