a) $a \equiv a \pmod{n}$ car $n \mid 0$ et $a - a = 0$. $\square$

b) $a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$

$\overset{4.2.1\ c)}{\Leftrightarrow} n \mid -(a-b)$

$\Leftrightarrow n \mid (b-a)$

$\Leftrightarrow b \equiv a \pmod{n}$ $\square$

c) $\left.\begin{array}{l} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{array}\right\} \Rightarrow n \mid (a-b)$ et $n \mid (b-c)$

$\overset{4.2.1\ d)}{\Rightarrow} n \mid [(a-b)+(b-c)]$

$\Rightarrow n \mid (a-c) \Rightarrow a \equiv c \pmod{n}$ $\square$

d) $a = q \cdot n + r \Rightarrow a - r = qn$

$\Rightarrow n \mid a - r \Rightarrow a \equiv r \pmod{n}$ $\square$

e) $\left.\begin{array}{l} a = q\cdot n + r \\ b = q'\cdot n + r \end{array}\right\} \Rightarrow a-b = (q-q')\cdot n$

$\Leftarrow$

$\Rightarrow n \mid (a-b)$

$\Rightarrow a \equiv b \pmod n$

$\Rightarrow$

$a \equiv b \pmod n \Rightarrow a - b = z\cdot n$

$\Rightarrow a = b + z\cdot n$

$\Rightarrow a = q\cdot n + \underbrace{r}_{\in [0;n[} + z\cdot n$

$\Rightarrow a = \overbrace{(q+z)}^{q'}\cdot n + r$

L'unicité de l'écriture $a = q'\cdot n + r$ avec $r \in [0;n[$ implique

$a \bmod n = b \bmod n$

f) $\left.\begin{array}{l} a \equiv c \pmod n \\ b \equiv d \pmod n \end{array}\right\} \Rightarrow \begin{array}{l} n \mid (a-c) \\ n \mid (b-d) \end{array}$

$$\Rightarrow n \mid [(a-c)+(b-d)]$$

$$\Rightarrow n \mid [(a+b)-(c+d)]$$

$$\Rightarrow a+b \equiv c+d \pmod n$$

Cela règle le cas de l'addition. Voyons ce qui est de la multiplication :

$$a - c = n \cdot y \qquad a = c + ny$$

$$b - d = n \cdot y' \qquad b = d + ny'$$

$$ab - cd = (c+ny)\cdot(d+ny') - cd$$

$$= \cancel{cd} + cny' + dny + n^2yy' - \cancel{cd}$$

$$= n\underbrace{(cy' + dy + nyy')}_{\in \mathbb{Z}}$$

Et donc, $ab \equiv cd \pmod{n}$

$\square$