Monitoria:

→ Ex (4 ii) e (6 i)

Ex (4 ii) Queremos que $a^{79} \equiv a \pmod{158}$

Temos que $158 = 2 \cdot 79$. Repare que

$a^{79} \equiv a \pmod{158} \iff 158 \mid a^{79} - a \iff$

$2 \cdot 79 \mid a^{79} - a$.

obs/ Se $mdc(a, b) = 1$, ∴

$a \mid c$ e $b \mid c \Rightarrow ab \mid c$

—//—

Usando a obs, basta provar que

$$\underbrace{2 \mid a^{79} - a}_{(2)} \quad \text{e} \quad \underbrace{79 \mid a^{79} - a}_{(1)}$$

(1) $79 \mid a^{79} - a \Leftrightarrow a^{79} \equiv a \pmod{79}$

Veja segue do cor. do teo. de fermat que $a^{79} \equiv a \pmod{79}$, já que 79 é primo.

(2) Note que

$$2 \mid a^{79} - a \iff \underbrace{a^{79} \equiv a \pmod 2}$$

Temos que, pelo alg. da divisão segue que

$$79 = 78 + 1 = 2 \cdot 39 + 1 \quad (*)$$

$$(79 = 2 \cdot 20 + 39 \text{ - tentativa Aline})$$

$$a^{79} = a^{2\cdot 39 + 1} = (a^2)^{39} \cdot a \equiv a^{39} \cdot a = a^{40}$$

$\pmod 2$, usando o cor. do teo. de Fermat.

Tente mostrar que $a^{40} \equiv a \pmod 2$ (Dica: use o cor. do teorema de Fermat).

Com isso, $a^{79} \equiv a \pmod{2}$

Logo, pelo obs anterior,

$$a^{79} \equiv a \pmod{158}$$

$\blacksquare$

—//—

Ex 6(i) Queremos encontrar r tal que

$$15! = 17q + r, \quad 0 \leq r < 17 \quad (*)$$

Usando a linguagem de congruências $(*)$ é equivalente à mostrar que $15! \equiv r \pmod{17}$

Note que pelo teorema de Wilson, para $p = 17$,

$$(17-1)! \equiv -1 \pmod{17} \iff$$

$$16! \equiv -1 \pmod{17} \iff$$

$$16 \cdot 15! \equiv -1 \pmod{17}$$

Veja que $16 \equiv -1 \pmod{17}$, logo

$$16 \cdot 15! \equiv -1 \pmod{17} \iff 15! \equiv 1 \pmod{17}$$

Daí, concluímos que $r = 1$. $\blacksquare$