Problema 3.7.16. *Demostrar que* $a^{560} \equiv 1$ *mód 561 para todo a con (a,561) = 1.*

Solución:

Por el Teorema de Euler-Fermat, sabemos que $a^{\phi(561)} \equiv 1$ mód 561 si (a,561)=1.

Ahora bien, $\phi(561) = \phi(3 \cdot 11 \cdot 17) = \phi(3) \cdot \phi(11) \cdot \phi(17) = 2 \cdot 10 \cdot 16 = 320$, luego $a^{320} \equiv 1$ mód 561, para todo a con (a,561)=1.

Pero si (a,561)=1, en particular (a,3)=1, (a,11)=1 y (a,17)=1, luego se tiene:

- $a^2 \equiv 1$ mód 3
- $a^{10} \equiv 1$ mód 11
- $a^{16} \equiv 1$ mód 17

Ahora bien, 560 = 320 + 240, luego tenemos que ver que $a^{240} \equiv 1$ módulo 561 para todo a tal que (a,561)=1. Para ello, basta ver si esa congruencia se cumple para los módulos 3, 11 y 17.

$$\left.\begin{array}{l} a^{240} \equiv a^{2^{120}} \equiv 1^{120} \equiv 1 \text{ mód } 3 \\ a^{240} \equiv a^{10^{24}} \equiv 1^{24} \equiv 1 \text{ mód } 11 \\ a^{240} \equiv a^{16^{15}} \equiv 1^{15} \equiv 1 \text{ mód } 17 \end{array}\right\}$$

$\Rightarrow a^{240} \equiv 1$ mód 561.

Por tanto:

$$a^{560} \equiv a^{320} \cdot a^{240} \equiv 1 \cdot 1 \equiv 1 \; mod \; 561$$

Problema escrito por Loly Soriano.