3.7.19. *Sea F_n un número de Fermat y p un primo. Demostrar que si p divide a F_n entonces $p = 2^{n+1}k + 1$ para algún entero k.*

Solución: Si p divide a F_n, tenemos que p es impar, ya que F_n lo es, y:

$$F_n = 2^{2^n} + 1 \equiv 0 \pmod{p}$$

O equivalentemente:

$$2^{2^n} \equiv -1 \pmod{p}$$

Elevando al cuadrado:

$$2^{2^{n+1}} \equiv 1 \pmod{p}$$

Concluímos que el orden de 2 en el grupo multiplicativo $\mathbb{Z}/p\mathbb{Z}$ es un divisor de 2^{n+1}, así que es de la forma 2^i, con $i \leq n+1$. Si el orden fuera menor que 2^{n+1}, llegaríamos a una contradicción, puesto que tendriamos $2^{2^n} \equiv 1 \not\equiv -1 \pmod{p}$.

Por el teorema de Lagrange, el orden de cualquier elemento divide al orden del grupo, que es $p-1$. Por tanto, $p - 1 = k2^{n+1}$, y $p = k2^{n+1} + 1$ para algún entero k.

Problema escrito por Rubén García-Valcárcel Sen