3.7.22. *Demostrar que existen infinitos primos de la forma* $4n+1$

Sea $n>1$ un entero, definimos $N=(n!)^2+1$. Sea p el menor divisor primo de N. Como N es impar, p no puede ser 2. Necesariamente p es mayor que n pues

$$p <= n \Rightarrow p \mid (n!)^2 = n^2 (n-1)^2 \ldots 2^2 1^2$$

y como $p \mid N=(n!)^2+1$ por hipótesis, tendríamos que $p \mid 1$.

Si demostramos que $p=4k+1$, podemos repetir el proceso reemplazando n por p y obtendríamos una sucesión infinita de primos de la forma $4k+1$.

Sabemos que p es de la forma $4k+1$ o $4k+3$. Como $p \mid N$, tenemos que

$$(n!)^2 \equiv -1 \mod p$$

y elevando a $\frac{p-1}{2}$ ambos lados tenemos

$$(n!)^{p-1} \equiv (-1)^{\frac{p-1}{2}} \mod p$$

y usando el Teorema 3.2.5 (Fermat) obtenemos

$$(-1)^{\frac{p-1}{2}} \equiv 1 \mod p$$

Si p fuese de la forma $4k+3$, tendríamos que $\frac{p-1}{2}=2k+1$ es impar, y por tanto, de la congruencia anterior sacaríamos que $-1 \equiv 1 \mod p$, lo cual sólo es posible si $p=2$, lo cuál contradice nuestra observación inicial.

Problema escrito por Óscar Losada Suárez