(2)

Tonyina

Proc: $p = 2^n + 1$; p primer $\Longrightarrow$ $n = 2^k$

Dem: contrarrecíproc: $n \neq 2^k \Longrightarrow p$ compost.

Farem contradicció en el contrarrecíproc:

Assumim $n \neq 2^k$ i $p = 2^n + 1$ primer.

$n \neq 2^k \Leftrightarrow n = 2^r \cdot q$ / amb q senar, $q > 1$.

$$p = 2^n + 1 = 2^{2^r \cdot q} + 1 = (2^{2^r})^q + 1^q \underset{q \text{ senar}}{=} (2^{2^r})^q - (-1)^q$$

$$= \underbrace{(2^{2^r} - (-1))}_{a = 2^{2^r} + 1} \underbrace{((2^{2^r})^{q-1} + \cdots + (-1)^{q-1})}_{b}$$

$\Longrightarrow p = ab$ amb $a > 1$ i $a < p$, pel que $b > 1$ i llavors p no és primer, el que és contradictori.

La contradicció implica que la hipòtesi no és possible i per tant queda demostrat que $p = 2^n + 1$ primer $\Longrightarrow n = 2^k$ ■