

Lema de Euclides: Para cada número primo p existe un número primo q tal que

$$p < q \leq 1 + p!$$

Demostración: Por reducción al absurdo.

Supongamos que existiera un número primo p_0 tal que ningún número primo q verificara la condición $p_0 < q \leq 1 + p_0!$ En ese caso tendríamos que

$$\forall x (p_0 < x \leq 1 + p_0! \rightarrow x \text{ no es primo})$$

En particular, el número $1 + p_0!$ **no** sería primo. Teniendo presente que p_0 es primo resulta que $1 + p_0! \geq 2$. Por tanto, el número $1 + p_0!$ admite una factorización en producto de números primos. Sea q_0 un número primo que interviene en la descomposición de $1 + p_0!$ Entonces se verifica:

- (a) $1 < q_0 < 1 + p_0!$
- (b) q_0 es un divisor de $1 + p_0!$
- (c) q_0 es un número primo.

Ahora bien, del hecho de que $q_0 < 1 + p_0!$ y de que q_0 sea un número primo, se deduce lo siguiente:

$$\left. \begin{array}{l} q_0 < 1 + p_0! \\ q_0 \text{ es un número primo} \\ \forall x (p_0 < x \leq 1 + p_0! \rightarrow x \text{ no es primo}) \end{array} \right\} \Rightarrow q_0 \leq p_0$$

Por tanto, si $q_0 \leq p_0$ entonces $q_0 \mid p_0!$ De donde se concluiría que q_0 no dividiría a $1 + p_0!$ Lo que contradice la condición (b).

■