Pequeño Teorema de Fermat y primos de Sophie Germain

Miguel Pineda Martín

March 2023

Los primos p para los que $2p+1$ es primo se conocen como primos de Sophie Germain. La siguiente proposición es una caracterización de dichos primos.

Proposición. Si p es primo, $q = 2p+1$ y se tiene que $2^{q-1} \equiv 1 \mod q$. Entonces, q es primo.

Demostración de la conjetura 1. Por reducción al absurdo, supongamos que q no es primo. El hecho de que:

$$2^{q-1} \equiv 1 \quad \text{mód } q$$

es equivalente a que $o(2) \mid q-1 = 2p$, donde $o(2)$ denota el orden de 2 en el grupo $(\mathbb{Z}/q\mathbb{Z})^*$. Ahora bien, esto implica que $o(2) \in \{2, p, 2p\}$. El primer caso no puede darse para $p \geq 2$ y, como el primer primo es el 2, dicho caso no puede darse. Supongamos que $o(2) = 2p$. Entonces, como q no es primo,

$$2p = o(2) \leq \varphi(q) < q-1 = 2p.,$$

lo cual es una contradicción. Por tanto, $o(2) = p$. Como $\varphi(q)$ es el orden del grupo $(\mathbb{Z}/q\mathbb{Z})^*$, $p = o(2) \mid \varphi(q) < 2p$. Por tanto, $\varphi(q) = p$. Ahora bien, si la factorización de q es $q = p_1^{a_1} \cdots p_r^{a_r}$, entonces

$$\varphi(q) = \prod_{i=1}^{r} (p^{a_i} - p^{a_i - 1}).$$

Lo cual implica que $\varphi(q)$ es par ya que todos los primos de la factorización de q son impares. Por tanto, $\varphi(q) = p = 2$, pero en este caso q es primo. De nuevo, una contradicción □