Sobre el Teorema de Navidad de Fermat

José Acevedo J.

Sea P un número primo tal que: $p \equiv 1 \ (mod\ 4)$, entonces p se puede expresar como la suma de dos cuadrados.

Ejemplos:

$5 - 1 = 4$, entonces: $5 = 2^2 + 1^2 = 4 + 1$

$13 - 1 = 12$, entonces: $13 = 2^2 + 3^2 = 4 + 9$

El teorema se cumple también para la resta de dos cuadrados, así tenemos que:

$5 - 1 = 4$, entonces: $5 = 3^2 - 2^2 = 9 - 4$

$13 - 1 = 12$, entonces: $13 = 7^2 - 6^2 = 49 - 36$

A pesar de que el teorema se cumple para ambos casos, es sólo el primero que recibe el nombre de teorema de Fermat sobre la suma de cuadrados o teorema de navidad, ya que Fermat mostró su teorema a Mersenne en una carta fechada el 25 de diciembre de 1640.

Dependiendo de la relación de los números primos con el modulo 4, estos pueden dividirse en dos grupos: los primos (p) y los primos (q).

1) Un número primo pertenece a p si:

$$p - 1 \equiv 0 \ (mod\ 4)$$

A este grupo pertenecen todos los números primos que se pueden expresar como la suma de dos cuadrados.

2) Un número primo pertenece a q si:

$$q + 1 \equiv 0 \ (mod\ 4)$$

Algunos números primos pertenecientes a este grupo son:

3, 7, 11, 19, 23…

A diferencia de los primos (p), que se pueden expresar como la suma y restas de dos cuadrados, los números primos (q) sólo pueden ser expresados como la diferencia o restas de dos cuadrados, así tenemos que:

3 + 1 = 4, entonces: $3 = 2^2 – 1^2$

7 + 1 = 8, entonces: $7 = 4^2 – 3^2$

$11 + 1 = 12$, entonces: $11 = 6^2 – 5^2$

$19 + 1 = 20$, entonces: $19 = 10^2 – 9^2$

$23 + 1 = 24$, entonces: $23 = 12^2 – 11^2$

Sea $m = 2x + 2$; y $n = 2x + 1$; tal que $x \geq 0$, si $(m + n\ + 1) \equiv 0\ (mod\ 4)$ entonces se cumple que:

$$m^2\ -\ n^2 = m + n$$