PRUEBA DE PRIMALIDAD .

Niceto Valcárcel Yeste. Licenciado en cc.físicas por la U.N.E.D.

October 27, 2011

1 Introducción.

Este estudio es una posible demostración de una condición de primalidad del tipo " si y sólo si ". El conocido Teorema de Wilson es una condición de primalidad de este tipo.

2 Proposición.

$(2m+1)$ es primo $\Longleftrightarrow \left(\frac{E\left(\frac{2m+1}{3}\right)!}{2m+1}\right)$ es número NO entero, donde $E\left(\frac{2m+1}{3}\right)$ es la parte entera del número $\left(\frac{2m+1}{3}\right)$.

2.1 Demostración.

.....$\Longrightarrow$) Si $(2m+1)$ es número primo, $\left(\frac{E\left(\frac{2m+1}{3}\right)!}{2m+1}\right)$ es número no entero.

Efectivamente, pues $(2m+1)$ y $\left(E(\frac{2m+1}{3})!\right)$, son coprimos.

$\Longleftarrow$) Si $\left(\frac{E\left(\frac{2m+1}{3}\right)!}{2m+1}\right)$ es no entero, $(2m+1)$ es número primo.

Para la demostración a continuación, por el método de reducción al absurdo, se considera " término " del factorial de un número $(n!)$ a cualquiera de los números naturales menores o iguales a él, es decir, $(n), (n-1), (n-2), ...3, 2, 1$.

Si $(2m+1)$ es un número compuesto, su mayor divisor primo posible es $E\left(\frac{2m+1}{3}\right)$, puesto que en el caso más desfavorable de ser $(2m+1)$ el producto de dos números primos, el menor posible de ellos es el 3, y en consecuencia, el mayor divisor primo posible es $E\left(\frac{2m+1}{3}\right)$.

Siendo $(2m+1)$ compuesto, sea $[(2m+1) = (2m_1+1)(2m_2+1)]$ cualquiera de sus posibles descomposiciones en producto de dos números. Ambos números son menores o iguales a $E\left(\frac{2m+1}{3}\right)$, máximo divisor posible de $(2m+1)$, y por tanto , " términos " del factorial $\left(E\left(\frac{2m+1}{3}\right)!\right)$, por lo que $\left(\frac{E\left(\frac{2m+1}{3}\right)!}{2m+1}\right)$ es número entero, a excepción, en principio, que sea $(m_1 = m_2)$, porque no hay dos términos iguales en el factorial. En este caso en el que $\left[2m+1 = (2m_1+1)^2\right]$, la

excepción persiste si $(2m_1+1)$ es un número primo, pues si fuera compuesto, $[(2m_1+1)=(2m_3+1)(2m_4+1)]$, existiría almenos otra descomposición en producto de dos números, $\left[(2m+1)=(2m_1+1)^2=(2m_3+1)^2(2m_4+1)^2\right]$, " términos " ambos del factorial $\left(E\left(\frac{2m+1}{3}\right)!\right)$, para la que se cumpliría que $\left(\frac{E\left(\frac{2m+1}{3}\right)!}{2m+1}\right)$, es número entero, incluso si es $(m_3=m_4)$, pues sería:

$\left[(2m+1)=(2m_1+1)^2=(2m_3+1)(2m_3+1)^3\right]$ una descomposición en producto de dos números distintos, " términos " ambos de $\left(E\left(\frac{2m+1}{3}\right)!\right)$.

Siendo por tanto $\left[(2m+1)=(2m_1+1)^2\right]$, el cuadrado de un número primo, $(2m_1+1)$ aparecerá con potencia mayor que 1 en $\left(E\left(\frac{2m+1}{3}\right)!\right)$, pues el factorial tiene, además del " término " $(2m_1+1)$, todos los " términos " en los que interviene $(2m_1+1)$ con cualquier otro número primo o compuesto menor que él, de forma que $\left(\frac{E\left(\frac{2m+1}{3}\right)!}{2m+1}\right)$ es siempre número entero.

Existe una única excepción, la de los dos primeros cuadrados, 3^2 y 5^2. En este caso son $\left[\frac{E\left(\frac{2m+1}{3}\right)!}{2m+1}=\frac{3!}{3^2}\right]$ y $\left[\frac{E\left(\frac{2m+1}{3}\right)!}{2m+1}=\frac{8!}{5^2}\right]$, números no enteros. Esta única excepción se debe al hecho de que $\left(E\left(\frac{3^2}{3}\right)=3\right)$ es menor que el primer múltiplo de 3, el 6; y $\left(E\left(\frac{5^2}{3}\right)=8\right)$ es menor que el primer múltiplo de 5, el 10. Ya en el siguiente número, el 7, es $\left(E\left(\frac{7^2}{3}\right)=16\right)$, mayor que el primer múltiplo de 7, el 14. En el siguiente número, el 9, es $\left(E\left(\frac{9^2}{3}\right)=27\right)$, mayor que el primer múltiplo de 9, el 18.

La excepción no resta generalidad a la proposición. Basta enunciarla, para una total generalidad, eliminando la excepción, así:

$(2m+1)$ es primo$\Longleftrightarrow\left(\frac{\left(E\left(\frac{2m+1}{3}\right)\right)!}{2m+1}\right)$ es número NO entero, para todo $\left(m\neq\left\{2^2;2^23\right\}\right)$.

2.1.1 Sea n cualquier número natural mayor que 0, distinto de $(2m+1)$ y distinto de cualquier múltiplo de $(2m+1)$.

$(2m+1)$ es primo $\Longleftrightarrow\frac{n\left(E\left(\frac{2m+1}{3}\right)!\right)}{2m+1}$ es número NO entero.

La demostración de esta propiedad es igual a la demostración de la sección 2. Basta decir que si $(2m+1)$ es primo, n es coprimo con él, cumpliéndose $(\Longrightarrow)$.

Si$(2m+1)$ es no primo, $\frac{n\left(E\left(\frac{2m+1}{3}\right)!\right)}{2m+1}$ es número entero, independientemente del valor de n, cumpliéndose $(\Longleftarrow)$.

3 Proposición.

Sea $(n!!)=(1)(3)(5)(7)\ldots\ldots\ldots$, el producto de los números impares de $(n!)$, que se denomina en este trabajo como factorial impar de (n).

$(2m+1)$ es primo $\Longleftrightarrow \left(\frac{E\left(\frac{2m+1}{3}\right)!!}{2m+1}\right)$ es número NO entero, donde $E\left(\frac{2m+1}{3}\right)$ es la parte entera del número $\left(\frac{2m+1}{3}\right)$ y $E\left(\frac{2m+1}{3}\right)!!$ es el factorial impar del número $E\left(\frac{2m+1}{3}\right)$.

3.1 Demostración.

La demostración es la misma que la de la sección 2.1 , puesto que fueron los " términos impares " del factorial de un número los que se emplearon para la demostración, siendo innecesarios los " términos pares " , salvo que la excepción de los cuadrados $\left\{3^2, 5^2\right\}$ se amplía a la de los cuadrados $\left\{3^2, 5^2, 7^2\right\}$ por ser $\left(9^2\right)$ el primer cuadrado con un múltiplo impar en: $(E\,(27)!!)$.

Como anteriormente, la excepción no resta generalidad a la proposición. Basta enunciarla así:

$(2m+1)$ es primo $\Longleftrightarrow \left(\frac{E\left(\frac{2m+1}{3}\right)!!}{2m+1}\right)$ es número NO entero, para todo $\left\{m \neq 2^2; 2^2 3; 2^3 3\right\}$.

3.1.1 Sea n cualquier número natural mayor que 0, distinto de $(2m+1)$ y distinto de cualquier múltiplo de $(2m+1)$.

$(2m+1)$ es primo $\Longleftrightarrow \frac{n\left(E\left(\frac{2m+1}{3}\right)!!\right)}{2m+1}$ es número NO entero.

La demostración de esta propiedad es igual a la demostración de la sección 2.1.1

Agradezco al lector el tiempo empleado, así como sus comentarios, que podrá enviarme a:

nicetovalcarcel@gmail.com