UNA CONDICIÓN DE PRIMALIDAD BASADA EN EL PEQUEÑO TEOREMA DE FERMAT.

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

October 17, 2011

1 Introducción.

Este trabajo es una posible demostración de una condición de primalidad del tipo " sí y sólo si " . El Teorema de Wilson es una condición de primalidad de este tipo, según la cual, un número $(2m+1)$ es primo, si y sólo si , es número entero el que resulta del cociente: $\frac{(2m)!+1}{2m+1}$.

La condición de primalidad objeto de este estudio se fundamenta en el pequeño teorema de Fermat. Este teorema dice que cualquier número natural a y cualquier número primo $(2m+1)$, coprimo con a , son tales que el cociente $\left(\frac{a^{2m}-1}{2m+1}\right)$, es número entero.

El propósito es obtener un número a , función de m , tal que si $(2m+1)$ es compuesto, el cociente $\left(\frac{a^{2m}-1}{2m+1}\right)$ nunca es número entero, y siempre es entero cuando $(2m+1)$ es número primo.

Concluye este estudio con una posible demostración del Teorema de Wilson, deducida de un caso particular de este mismo trabajo.

2 Proposición.

Un número $(2m+1)$, para todo $m \in IN - \{0\}$, es número primo, sí y sólo si, es número entero el que resulta del conciente:

$\frac{(\prod(\frac{2m+1}{3}))^{2m}-1}{2m+1}$, siendo:

$\prod(\frac{2m+1}{3})$, el producto o productorio de los números primos menores o iguales a $(\frac{2m+1}{3})$.

2.1 Demostración.

.

$\Longrightarrow$) Si $(2m+1)$ es número primo, $\prod\left(\frac{2m+1}{3}\right)$ es coprimo con él, de manera que según el pequeño teorema de Fermat, $\left(\frac{\left(\prod\left(\frac{2m+1}{3}\right)\right)^{2m}-1}{2m+1}\right)$ es número entero.

$\Longleftarrow$) Si $\left(\frac{\left(\prod\left(\frac{2m+1}{3}\right)\right)^{2m}-1}{2m+1}\right)$ es número entero, $(2m+1)$ es número primo, como se demuestra a continuación, por el método de reducción al absurdo.

Si $(2m+1)$ es número no primo, no puede tener divisores primos mayores que $E\left(\frac{2m+1}{3}\right)$, donde $E\left(\frac{2m+1}{3}\right)$ es la parte entera de $\left(\frac{2m+1}{3}\right)$, pues al ser compuesto es, en el caso más desfavorable, el producto de dos números primos. Siendo el menor posible de ellos el 3, el mayor divisor primo posible es $E\left(\frac{2m+1}{3}\right)$.

Sea $(2m+1)=(p_1^{a_1}....p_i^{a_i}....p_n^{a_n})$, la descomposición factorial de un número compuesto cualquiera. En tal caso:

$(2m)=(p_1^{a_1}....p_i^{a_i}....p_n^{a_n}-1)$.

Todos los números primos $(p_1,..p_i..,p_n)$ que forman parte de la descomposición factorial de $(2m+1)$ son números del productorio $\prod\left(\frac{2m+1}{3}\right)$.

Dado que el productorio se encuentra elevado a $(2m)$, es número entero el cociente:

$$\frac{\left(\prod\left(\frac{2m+1}{3}\right)\right)^{2m}}{2m+1}=\frac{\left(\prod(p_j)\right)^{2m}(p_1....p_i...p_n)^{\left(p_1^{a_1}.....p_i^{a_i}....p_n^{a_n}-1\right)}}{p_1^{a_1}p_2^{a_2}.....p_n^{a_n}}=$$

$$=\left(\prod(p_j)\right)^{2m}p_1^{\left(p_1^{a_1}..p_i^{a_i}...p_n^{a_n}-1-a_1\right)}....p_i^{\left(p_1^{a_1}...p_i^{a_i}...p_n^{a_n}-1-a_i\right)}....p_n^{\left(p_1^{a_1}....p_i^{a_i}....p_n^{a_n}-1-a_n\right)}$$

pues cualquier exponente $(p_1^{a_1}..p_i^{a_i}..p_n^{a_n}-1-a_i)$ de cualquier número primo p_i de la citada descomposición factorial, es mayor que 0.

$\prod(p_j)$ es el productorio de los números primos de $\prod\left(\frac{2m+1}{3}\right)$ que no forman parte de la descomposición factorial de $(2m+1)$.

Finalmente, $\left(\frac{1}{2m+1}\right)$ no es número entero, y en consecuencia, $\left(\frac{\left(\prod\left(\frac{2m+1}{3}\right)\right)^{2m}-1}{2m+1}\right)$ sería número no entero.

3 Propiedades.

1ª) Aplicación de lo demostrado en la sección anterior a los números mayores que 3.

Como es sabido, todos los números primos mayores que 3 , son de una de las dos formas siguientes: $(6n\pm1)$.

Un número $(6n+1)$, para todo $n\in IN-\{0\}$, es número primo sí y sólo si es número entero el que resulta del conciente$\left(\frac{\left(\prod\left(\frac{6n+1}{5}\right)\right)^{6n}-1}{6n+1}\right)$.

Un número $(6n-1)$, para todo $n\in IN$-$\{0\}$, es número primo sí y sólo si es número entero el que resulta del conciente$\left(\frac{\left(\prod\left(\frac{6n-1}{5}\right)\right)^{6n-2}-1}{6n-1}\right)$,

siendo$\prod\left(\frac{6n\pm1}{5}\right)$, el productorio de los números primos menores o iguales a $\left(\frac{6n\pm1}{5}\right)$ y mayores o iguales a 5.

Atendiendo a lo demostrado en la sección anterior, y dado que los valores de m son todos los pertenecientes a los conjuntos:

$m = \{3n-1\} = \{2, 5, 8, 11.....\infty\}$
$m = \{3n\} = \{3, 6, 9, 12, 15, ...\infty\}$
$m = \{3n+1\} = \{4, 7, 10, ...\infty\}$
pueden descartarse todos los números del conjunto $\{3n+1\}$ de la prueba de primalidad, porque para todos ellos es:
$(2m+1) = 3\,(2n+1)$, número no primo.
Haciendo $(m = 3n+1)$ en $\left(\frac{(\prod(\frac{2m+1}{3}))^{2m}-1}{2m+1}\right)$, se obtiene:
$\left(\frac{(\prod(2n+1))^{2(3n+1)}-1}{3(2n+1)}\right)$, que siempre es número no entero, por ser siempre entero el número $\left(\frac{(\prod(2n+1))^{2(3n+1)}}{3(2n+1)}\right)$, y nunca el número $\left(\frac{1}{3(2n+1)}\right)$.
Para el resto de valores de m, ($m = \{3n\}$ y $m = \{3n-1\}$) ,
$(2m+1)$ no será múltiplo de 3, de forma que no será 3 el mínimo divisor posible de $(2m+1)$ sino 5, y no será $E\left(\frac{2m+1}{3}\right)$ el máximo divisor posible de $(2m+1)$, sino $E\left(\frac{2m+1}{5}\right)$.
Haciendo $(m = 3n)$ en $\left(\frac{(\prod(\frac{2m+1}{5}))^{2m}-1}{2m+1}\right)$, resulta: $\left(\frac{(\prod(\frac{6n+1}{5}))^{6n}-1}{6n+1}\right)$
Haciendo $(m = 3n-1)$ en $\left(\frac{(\prod(\frac{2m+1}{5}))^{2n}}{2m+1}\right)$, resulta: $\left(\frac{(\prod(\frac{6n-1}{5}))^{6n-2}-1}{6n-1}.\right)$
.
$2^{\underline{a}}$)
Sean $(n_1, n_2) \in IN - \{0\}$, cualesquiera números naturales mayores que 0, y tales que $[n_1 \neq n_2\,(2m+1)]$, para todo $m \in IN - \{0\}$; es decir, sea n_1 cualquier número natural mayor que 0, distinto de $(2m+1)$ y distinto de cualquier múltiplo de $(2m+1)$.
El número $(2m+1)$ es primo $\Longleftrightarrow$ es número entero el que resulta del conciente$\left(\frac{(n_1\prod(\frac{2m+1}{3}))^{2m}-1}{2m+1}\right)$.
La demostración de esta propiedad es igual a la demostración de la sección 2. Basta decir que si $(2m+1)$ es número primo, n_1 es coprimo con él, cumpliéndose la implicación $(\Longrightarrow)$; y si$(2m+1)$ es no primo, $\left(\frac{(n_1\prod(\frac{2m+1}{3}))^{2m}-1}{2m+1}\right)$ es número no entero, independientemente del valor de n_1, cumpliéndose la implicación $(\Longleftarrow)$

4 Proposición.

El Teorema de Wilson puede deducirse apartir del resultado anterior para el caso particular:
$n_1 = \frac{(2m)!}{(\prod(\frac{2m+1}{3}))}$

4.1 Demostración.

Según la propiedad $(2^{\underline{a}})$, siendo:

$n_1 = \frac{(2m)!}{(\prod(\frac{2m+1}{3}))}$.

puede enunciarse:

$(2m+1)$ es primo $\Longleftrightarrow$ es número entero el que resulta del conciente$\Big(\frac{((2m)!)^{2m}-1}{2m+1}\Big)$.

Ahora bien,

$\frac{((2m)!)^{2m}-1}{2m+1} = \frac{((2m)!+1)\big(((2m)!)^{2m-1}-((2m)!)^{2m-2}+...+(2m)!-1\big)}{2m+1}$

.

Si $(2m+1)$ es compuesto, los dos miembros de la igualdad son números no enteros, y en consecuencia, $\frac{(2m)!+1}{2m+1}$ es número no entero.

Si $(2m+1)$ es primo, los dos miembros de la igualdad son números enteros, y en consecuencia, $\frac{(2m)!+1}{2m+1}$ es número entero puesto que $\frac{((2m)!)^{2m-1}-((2m)!)^{2m-2}+...+(2m)!-1}{2m+1}$ no es número entero, como se demuestra a continuación.

Al ser:

.

$\frac{(2m)!}{2m+1} = c + \frac{r}{2m+1}$

donde c es el cociente de la división, r, el resto de la división, ($0 < r \leq 2m$ por ser $(2m+1)$ número primo), se desprende:

$(2m)! = c\,(2m+1) + r$

que sustituído en:

.

$\frac{((2m)!)^{2m-1}-((2m)!)^{2m-2}+...+(2m)!-1}{2m+1}$

resulta:

.

$\frac{((2m+1)c+r)^{2m-1}-((2m+1)c+r)^{2m-2}+...+(2m+1)c+r-1}{2m+1} = N + \frac{r^{2m-1}-r^{2m-2}+...+r-1}{2m+1}$

.

donde N es el número natural que se obtiene, una vez realizados los desarrollos de Newton de los binomios y eliminado el factor común $(2m+1)$, pues el propósito es averiguar cuándo es número entero el cociente, es decir, cuándo es número entero el que resulta de:

$\frac{r^{2m-1}-r^{2m-2}+...+r-1}{2m+1} = \frac{\frac{r^{2m}-1}{r+1}}{2m+1} = \frac{r^{2m}-1}{(r+1)(2m+1)}$

1º) Por un lado, $\frac{r^{2m}-1}{r+1}$ es número entero pues es la suma de una progresión geométrica de razón entera y con el primer término de la progresión, también número entero. De ello se deriva que $\big(r^{2m}-1\big)$ contiene a $(r+1)$ en su descomposición factorial.

2ª) Por otro lado, $\frac{r^{2m}-1}{2m+1}$ es número entero pues $(2m+1)$ es primo y r es coprimo con él.(pequeño teorema de Fermat). De ello se deriva que $\big(r^{2m}-1\big)$ contiene a $(2m+1)$ en su descomposición factorial.

Ambas cosas sugieren, en principio, que no sea obligado que deba ser número entero $\Big(\frac{(2m)!+1}{2m+1}\Big)$ por ser entero el número $\Big(\frac{r^{2m}-1}{(r+1)(2m+1)}\Big)$, cuando $(2m+1)$ es número primo, salvo si es $(r = 2m)$, pues $\big(r^{2m}-1\big)$ no tiene por qué contener a $(r+1) = (2m+1)$ en su descomposición factorial elevado al cuadrado, y consecuentemente hay que demostrar cuándo es $\Big(\frac{(2m)^{2m}-1}{(2m+1)^2}\Big)$ número entero, siendo $(2m+1)$, número primo.

La respuesta es " nunca " . El número $\left((2m)^{2m}-1\right)$ tiene al número primo $(2m+1)$ en su descomposición factorial (pequeño teorema de Fermat), pero no elevado al cuadrado, como se demuestra a continuación, por el método de reducción al absurdo:

Sea $\left(e_1=\frac{a^a-1}{(a+1)^2}=\frac{a^{a-1}-a^{a-2}+...-a^2+a-1}{a+1}\right)$, número entero con $(a=2m)$. Debe tenerse presente que a es número par en lo que sigue.

$e_1+1=e_2=\frac{a^{a-1}-a^{a-2}+...+a-1}{a+1}+1=a\frac{a^{a-2}-a^{a-3}+...-a+2}{a+1}$

Al ser coprimos (a) y $(a+1)$, debe ser entero:

$e_3=\frac{e_2}{a}=\frac{a^{a-2}-a^{a-3}+...+a^2-a+2}{a+1}\Longrightarrow e_3-2=e_4=\frac{a^{a-2}-a^{a-3}+...-a+2}{a+1}-2=$

$=a\frac{a^{a-3}-a^{a-4}+...+a-3}{a+1}$

Al ser coprimos (a) y $(a+1)$, debe ser entero:

$e_5=\frac{e_4}{a}=\frac{a^{a-3}-a^{a-4}+...+a-3}{a+1}\Longrightarrow e_5+3=e_6=\frac{a^{a-3}-a^{a-4}+...+a-3}{a+1}+3=$

$=a\frac{a^{a-4}-a^{a-5}+...-a+4}{a+1}$

Al ser coprimos (a) y $(a+1)$, debe ser entero:

$e_7=\frac{e_6}{a}=\frac{a^{a-4}-a^{a-5}+...-a+4}{a+1}\Longrightarrow e_7-4=e_8=\frac{a^{a-4}-a^{a-5}+...-a+4}{a+1}-4=$

$=a\frac{a^{a-5}-a^{a-6}+...+a-5}{a+1}$

Así sucesivamente hasta obtener que debe ser número entero:

$\frac{a^{a-(a-2)}-a^{a-(a-1)}+(a-2)}{a+1}=\frac{a^2-a+(a-2)}{a+1}=\frac{a^2-2}{a+1}=\frac{\left(a^2-1\right)-1}{a+1}=$

$=a-1-\frac{1}{a+1}=2m-1-\frac{1}{2m+1}$

que es número entero sólo para $(m=0)$

Queda pues demostrada la proposición.

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

nicetovalcarcel@gmail.com

.

Dedico este estudio, con mi más sincero agradecimiento, al personal del Hospital Perpetuo Socorro de Albacete, a quienes admiro por su profesionalidad, su humanidad, y su generosísima dedicación.