PROPIEDAD DE LOS NÚMEROS PRIMOS DE FERMAT.

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

June 26, 2011

1 Introducción.

Este trabajo muestra que los números primos de Fermat, es decir, los números primos de la forma $2^{2^n}+1$ son los únicos números primos de la forma 2^m+1 , para todo número natural $m>0$.

El trabajo se apoya en el conjunto de los números impares no primos. Como demostraré, este conjunto está fielmente representado por una función que llamo función generadora de los números impares no primos. Es una función completamente general, sin particularidades de ninguna clase.

Sin más preámbulo, comienzo.

2 El conjunto de los números impares no primos.

2.1 Proposición.

El conjunto de los números impares no primos (en adelante, números compuestos) es el representado por la expresión:

$2m+1=(2x+1)(2y+1)=2(2xy+x+y)+1$

donde x e y son cualesquiera pareja de números naturales mayores que 0.

Es $m=2xy+x+y$ la función generadora de los números impares no primos, que es al mismo tiempo, el conjunto de los números naturales a partir del cual se obtienen todos los números impares no primos, sin más que multiplicándolos por 2 y sumando 1 al resultado.

2.2 Demostración.

Si $2m+1$ es un número compuesto, es almenos el producto de dos números distintos de 1. Si es el producto de más de dos números, la propiedad asociativa del producto siempre podrá convertirlo en un producto de dos números.

Por otro lado, el producto de dos números con la condición impuesta, es siempre un número compuesto.

3 Proposición.

Los números primos de Fermat, es decir, los números primos de la forma $2^{2^n}+1$,son los únicos primos de la forma 2^m+1 , para todo número natural $m>0$.

3.1 Demostración.

Un número de la forma 2^m+1 es compuesto si existen dos números naturales mayores que 0, x e y , para los que se cumple:

$2^{m-1}=2xy+x+y$

Ha de ser necesariamente:

$x+y=2z$

Sustituyendo:

$2^{m-2}=x\left(2z-x\right)+z=2zx+z-x^2$

Sea:

$z=x^2\Longrightarrow y=2x^2-x$

$2^{m-3}=x^3$

Por tanto, si m es múltiplo de 3, $m=3k$, para todo $k>0$, se cumplirá:

$x=2^{k-1}\Longrightarrow y=2^{2k-1}-2^{k-1}$

resultando:

$2^{3k}+1=\left(2^k+1\right)\left(2^{2k}-2^k+1\right)$

Si en lugar de ser:

$z=x^2$

es:

$z-x^2=2z_1$

resulta:

$2^{m-3}=x\left(2z_1+x^2\right)+z_1=2z_1x+z_1+x^3$

Haciendo ahora:

$z_1+x^3=2z_2$

resulta:

$2^{m-4}=x\left(2z_2-x^3\right)+z_2=2z_2x+z_2-x^4$

Sea:

$z_2=x^4\Longrightarrow y=2z-x=2\left(2z_1+x^2\right)-x=2\left(2\left(2z_2-x^3\right)+x^2\right)-x=2\left(2\left(2x^4-x^3\right)+x^2\right)-x$

$2^{m-5}=x^5$

Al igual que anteriormente, si m es múltiplo de 5, $m=5k$, para todo $k>0$, se cumplirá:

$x=2^{k-1}\Longrightarrow y=2\left(2\left(2\left(2^{k-1}\right)^4-\left(2^{k-1}\right)^3\right)+\left(2^{k-1}\right)^2\right)-2^{k-1}$

resultando:

$2^{5k}+1=\left(2^k+1\right)\left(4\left(2\left(2\left(2^{k-1}\right)^4-\left(2^{k-1}\right)^3\right)+\left(2^{k-1}\right)^2\right)-2^k+1\right)$

Procediendo de la misma manera se obtendría:

$2^{m-7}=x^7$

si m es múltiplo de 7, $m=7k$, para todo $k>0$, se cumpirá:

$x=2^{k-1}$, y su correspondiente y.

Siguiendo el mismo procedimiento se obtendría para cualquier $m=\left(2q_1+1\right)k$

Todos los números de la forma $2^{(2q_1+1)k}+1$, para todo q_1, k naturales mayores que 0 son divisibles por el número 2^k+1.

Resulta entonces que todos los números de la forma 2^m+1 son números no primos cuando m es cualquier número impar mayor que 1 o cualquier múltiplo de cualquier número impar mayor que 1.

El conjunto complementario de este conjunto m , respecto del conjunto de los números naturales, es el formado por los números de la forma 2^n , para todo $n>0$.

Así pues, los números primos de la forma 2^m+1 que existen, son números primos de la forma $2^{2^n}+1$, es decir, números primos de Fermat.

Por otro lado el número 2^k+1, divisor del número $2^{(2q+1)k}+1$, es también un número de la forma 2^m+1 ,pudiendo cumplirse:

Si $k=1$, el número 2^m+1 es múltiplo de $3=2^1+1$

Si $k=2^n$, para todo $n>0$, el número 2^k+1 podrá ser primo.

Si $k=(2q_1+1)\,2^n$, el número 2^k+1 , no será primo, por ser divisible por el número, $2^{2^n}+1$.

Si $k=(2q_1+1)$, el número 2^k+1 nunca será primo. En este caso, volveríamos a proceder de la misma manera haciendo $k=m$.

Este trabajo ha sido realizado por Niceto Valcárcel Yeste, licenciado en cc.físicas por la U.N.E.D.

Agradezco al lector el tiempo empleado, y sus comentarios, que podrá enviarme a la dirección de correo electrónico:

nicetovalcarcel@gmail.com