EL TEOREMA DE WILSON Y LA INFINITUD DE LOS NÚMEROS PRIMOS.

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

September 21, 2011

1 Introducción.

El teorema de Wilson es la única condición de primalidad directa que se conoce. Para saber si un número n es primo basta con saber si es número entero el que resulta de $\left(\frac{(n-1)!+1}{n}\right)$. Si ese cociente no es entero, el número no es primo. Si el cociente es entero, el número es primo. Formalmente:

n es primo $\Longleftrightarrow \frac{(n-1)!+1}{n} \in E$, siendo E el conjunto de los números naturales impares.

Una condición de primalidad permite averiguar si un número es o no primo. Todas las maneras conocidas, excepto este teorema y las propiedades que se derivan de él, son indirectas.

Formas indirectas de averiguar si un número es o no primo son:

-Dividir por sus posibles divisores primos.

-Averiguar si el número puede expresarse de forma única como diferencia de cuadrados. En tal caso, el número es primo. Si existe más de una manera de expresar al número como diferencia de cuadrados, el número es compuesto.

-Apartir del teorema de Fermat, para los primos de la forma $(4n+1)$, es decir, comprobar si el número $(4n+1)$ puede expresarse de forma única como suma de cuadrados, en cuyo caso el número es primo; en caso contrario, el número es compuesto.

El conocido como pequeño teorema de Fermat, no es una condición de primalidad. Según este teorema, si p es primo y a es cualquier número natural coprimo con p (p y a son coprimos si no tienen factores primos comunes en su descomposición factorial), ha de ser número entero el que resulta de $\left(\frac{a^{p-1}-1}{p}\right)$. Si el cociente no es entero, p no es primo, pero si el cociente es entero no se asegura que p sea número primo, porque todos los números primos cumplen el teorema, pero también lo cumplen números no primos.

Se concluye la introducción indicando que no se utiliza en este trabaj0 ningún conocimiento que implique directa o indirectamente la infinitud del conjunto de los números primos, porque se piensa que se ha podido conseguir bajo este precepto. De no haber podido ser así, son perfectamente válidos cualesquiera conocimientos, sobretodo si no se encuentra otro camino, pero utilizados de

forma correcta, lo que puede ser delicado, como por ejemplo ocurre en uno de los pasos de esta demostración, que podría quizá haberse resuelto apoyándose en el teorema de Bertrand-Chevychov, utilizando de él, el hecho de existir un número primo en el intervalo $(n; 2n)$; pero el teorema dice a este respecto, para cualquier n , lo que implica directamente la infinitud de los números primos; precísamente lo que se pretende demostrar.

Este estudio es una posible demostración de la infinitud de los números primos desarrollada por completo apartir de este maravilloso TEOREMA DE WILSON.

2 Proposición.

Existen infinitos números primos.

2.1 Demostración.

Sea n cualquier número primo, y sea $(2e + 1)$ el número entero que resulta de:

$\frac{(n-1)!+1}{n} = 2e + 1$

$(n - 1)! + 1 = n\,(2e + 1)$.

Se considera " factor primo " de un número impar a cualquiera de los números primos que forman parte de su descomposición factorial.

Los factores primos de $(2e + 1)$ han de ser mayores o iguales a n , pues si no fuera así, siendo $(2e_1 + 1)$ uno cualquiera de ellos:

$\frac{(n-1)!+1}{2e_1+1} + \frac{1}{2e_1+1} = \frac{2e+1}{2e_{1+1}}\ n$

esta igualdad nunca se cumpliría, pues $\frac{(n-1)!+1}{2e_1+1}$ y $\frac{2e+1}{2e_{1+1}}$ son enteros, mientras que $\frac{1}{2e_1+1}$, no lo es.

Por otro lado, si $(2e + 1)$ es primo, ha de ser mayor o igual que n, pues en caso contrario sería:

$\frac{(n-1)!+1}{2e+1} + \frac{1}{2e+1} = n$, donde $\frac{(n-1)!+1}{2e+1}$ es entero mientras $\frac{1}{2e+1}$, no lo es.

El hecho de que los factores primos de $(2e + 1)$ deban ser mayores o iguales al número primo n elegido, es ya una demostración de la infinitud del conjunto de los números primos, excepcto que fuera para un n:

$(n - 1)! + 1 = n^a$, con a un número natural.

Encontrar un n y un a que cumplan esta condición, implica que el razonamiento anterior no es válido para demostrar la infinitud del conjunto de los números primos, salvo que pudiera demostrarse la existencia de un número primo, $(n + 2k) > n$, para el que no se cumpla:

$(n + 2k - 1)! + 1 = (n + 2k)^b$

siendo b número natural .

2.1.1 Demostración por reducción al absurdo.

Se supone que existe un último número primo n para el que existe un a tal que:

$(n - 1)! + 1 = n^a$

1º) sea $a = 2a_0 + 1$, un número impar. Sumando 1 a ambos miembros de la ecuación, y sustituyendo, resulta:

$(n-1)! + 2 = n^{2a_0+1} + 1 = (n+1)\left(n^{2a_0} - n^{2a_0-1} + \ldots\ldots - n + 1\right)$

Esta igualdad no puede cumplirse pues los factores primos, en su caso, de $(n+1)$ se encuentran en $(n-1)!$, y si $(n+1) = 2^\alpha$, con α un número natual cualquiera, debería ser $\alpha = 1$, pues $(n-1)! = 2^\beta (2k+1)$, con β un número natual mayor que 1.

Por tanto, no puede ser a un número impar.

2º) Sea $a = 2^\alpha (2a_0 + 1)$, un número par.

$(n-1)!+2 = n^{2^\alpha(2a_0+1)}+1 = \left(n^{2^\alpha}\right)^{2a_0+1}+1 = \left(n^{2^\alpha}+1\right)\left(\left(n^{2^\alpha}\right)^{2a_0} - \left(n^{2^\alpha}\right)^{2a_0-1} + \ldots - n^{2^\alpha} + 1\right)$

Esta igualdad no puede cumplirse pues los factores primos, en su caso, de $\left(n^{2^\alpha}+1\right)$ se encuentran en $(n-1)!$, y si $\left(n^{2^\alpha}+1\right) = 2^{\alpha_1}$, con α_1 un número natual cualquiera, debería ser $\alpha_1 = 1$, pues $(n-1)! = 2^\beta (2k+1)$, con β un número natual mayor que 1.

Sólo es posible que sea $a_0 = 0$

En tal caso, sea $n = 2n_0 + 1$

Ha de cumplirse, utilizando el binomio de Newton:

$(2n_0)!+1 = (2n_0+1)^{2^\alpha} = \binom{2^\alpha}{0}(2n_0)^{2^\alpha} + \binom{2^\alpha}{1}(2n_0)^{2^\alpha-1} + \ldots + \binom{2^\alpha}{2^\alpha-1} 2n_0 + 1$

$(2n_0-1)! = \binom{2^\alpha}{0}(2n_0)^{2^\alpha-1} + \binom{2^\alpha}{1}(2n_0)^{2^\alpha-2} + \ldots + \binom{2^\alpha}{2^\alpha-2} 2n_0 + \binom{2^\alpha}{2^\alpha-1}$

$(2n_0-1)! = \binom{2^\alpha}{0}(2n_0)^{2^\alpha-1} + \binom{2^\alpha}{1}(2n_0)^{2^\alpha-2} + \ldots + \binom{2^\alpha}{2^\alpha-2} 2n_0 + 2^\alpha$

$(2n_0-1)! - 2^\alpha = 2n_0\left[\binom{2^\alpha}{0}(2n_0)^{2^\alpha-2} + \binom{2^\alpha}{1}(2n_0)^{2^\alpha-3} + \ldots + \binom{2^\alpha}{2^\alpha-2}\right]$

Esta igualdad es cierta sólo si, $n_0 = 2^\beta$, pues los factores primos, en su caso, de n_0 se encuentran en $(2n_0-1)!$.

Sea $n = 2^{\beta+1} + 1$.

Para este valor de n , utilizando la propiedad " suma por diferencia igual a diferencia de cuadrados " :

$\left(2^{\beta+1}\right)! = \left(2^{\beta+1}+1\right)^{2^\alpha} - 1 = \left(2^{\beta+1}+2\right)^{2^{\alpha-1}}\left(2^{\beta+1}\right)^{2^{\alpha-1}} = \left(2^\beta+1\right)^{2^{\alpha-1}}\left(2^{\beta+2}\right)^{2^{\alpha-1}}$

Esta última igualdad es falsa (excepto para $\alpha = \beta = 1$), como se demuestra a continuación, basándose en el obligado cumplimiento de la paridad de la igualdad, es decir, la potencia de 2 en ambos miembros, ha de ser igual.

$\left(2^{\beta+1}-1\right)! = \left(2^\beta+1\right)^{2^{\alpha-1}}\left(2^{\beta+1}\right)^{\left(2^{\alpha-1}-1\right)} 2^{2^{\alpha-1}}$.

El número de términos pares en $\left(2^{\beta+1}-1\right)!$, es:

$\frac{2^{\beta+1}-2}{2} = 2^\beta - 1$,

y los términos son:

$\left(2^{\beta+1}-2\right)\left(2^{\beta+1}-4\right)\left(2^{\beta+1}-6\right)\left(2^{\beta+1}-8\right)\ldots\left(2^{\beta+1}-\left(2^{\beta+1}-4\right)\right)\left(2^{\beta+1}-\left(2^{\beta+1}-2\right)\right)$

De ellos,

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

son el producto de 2 por un número impar, y se presentan alternativamente en la expresión anterior, desde el primero hasta el último.

Son por tanto $\left(2^{\beta-1}\right)$ términos, de los que se obtiene la potencia de 2 , $\left(2^{2^{\beta-1}}\right)$.

.

.

Quedan pues,

$\left(2^{\beta}-1-2^{\beta-1}=2^{\beta-1}-1\right)$, términos pares; los siguientes:

$\left(2^{\beta+1}-4\right)\left(2^{\beta+1}-8\right)\left(2^{\beta+1}-12\right).....\left(2^{\beta+1}-\left(2^{\beta+1}-8\right)\right)\left(2^{\beta+1}-\left(2^{\beta+1}-4\right)\right)$

De ellos,

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

son el producto de 4 por un número impar, y se presentan alternativamente en la expresión anterior, desde el primero hasta el último.

Por consiguiente, la potencia de $\left(4=2^2\right)$ es, $\left(2^{2^{\beta-2}}\right)$, y la correspondiente potencia de 2, $\left(2^{2\left(2^{\beta-2}\right)}\right)$.

De la misma manera se obtendría la potencia de $\left(8=2^3\right)$, $\left(2^{2^{\beta-3}}\right)$, y la correspondiente de 2, $\left(2^{3\left(2^{\beta-3}\right)}\right)$.

Se comprueba, como suma de una progresión geométrica, que el número total de términos pares es:

$2^{\beta}-1=2^{\beta-1}+2^{\beta-2}+2^{\beta-3}+.....+2^2+2+1=\frac{1-2^{\beta}}{1-2}$

(El 1 de la suma anterior corresponde al último término de la criva; el del medio, $\frac{2^{\beta+1}-1+1}{2}=2^{\beta}$).

Así sucesivamente se concluye la potencia final para 2:

$2^{1\left(2^{\beta-1}\right)+2\left(2^{\beta-2}\right)+3\left(2^{\beta-3}\right)+.....+(\beta-2)\left(2^{\beta-(\beta-2)}\right)+(\beta-1)2+\beta}=2^{\sum_{i=1}^{i=\beta} i\left(2^{\beta-i}\right)}$

El sumatorio puede sumarse como progresión aritmético-geométrica:

$\sum_{i=1}^{i=\beta}\left(i2^{\beta-i}\right)=1\left(2^{\beta-1}\right)+2\left(2^{\beta-2}\right)+\ldots+(\beta-1)2+\beta=2^{\beta+1}-\beta-2$.

obteniéndose:

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

Igualando los exponentes:

$2^{\beta+1}-\beta-2=(\beta+1)\left(2^{\alpha-1}-1\right)+2^{\alpha-1}$

$2^{\beta+1}-1=(\beta+1)2^{\alpha-1}+2^{\alpha-1}=(\beta+2)2^{\alpha-1}$

por lo que $\alpha=\beta=1$,

pues $\left((\beta+2)2^{\alpha-1}\right)$ ha de ser impar, por serlo $\left(2^{\beta+1}-1\right)$,

y así debe ser $\alpha=1\Longrightarrow\beta=1$

$2^2!+1=\left(2^2+1\right)^2=5^2$.

El conjunto de los números primos, según este estudio, contiene infinitos números.

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

nicetovalcarcel@gmail.com