# **¿Como saber si un número es primo?**

**No** es una tarea **trivial** determinar si **un número es primo** o no. Saber si un número es primo siempre ha atraído fuertemente a los matemáticos y aficionados que han obtenido algunos **éxitos parciales**; pero **nadie** ha obtenido aún una fórmula matemática exacta y de tiempo y estructura algorítmica aceptable que **resuelva** esta pregunta **para todos** o un conjunto indefinido de números primos.

Un número es primo si no es múltiplo o divisible por otro número que no sea el mismo y la unidad.

Si queremos saber si un número es primo, podemos probar de **dividir** entre 1,2,3,4…. hasta el número, si **ninguno** de ellos lo divide, el número será **primo**.

Esta idea aparece en el siguiente dibujo que se conoce con el nombre de máquina de Conway (Jhon Horton), matemático inglés de la Universidad de Cambridge, representado en la figura dando pedales para que funcione la máquina. El grupo de inspectores comprueba si el número que pasa por la cadena es divisible por el que tiene asignado y en caso afirmativo lo rechaza.  
  
El problema es que tenemos que probar tantos números como el número sea de grande, por lo que podemos mejorar la estrategia.  
  
Sabemos que si un número es divisible o múltiplo de otro, entonces cualquier producto de ese número también lo és.  
Por esto si dividimos por un número compuesto (que es el producto de al menos un primo), será divisible también por este primo, por eso:  
  
Para saber si un número es primo basta con mirar si es divisible entre algún primo hasta el número.  
  
Pero… ¿Es necesario mirar todos los números primos hasta el número?  
  
Tampoco, si nos fijamos cuando probamos en orden los números primos, los estamos descartando por orden, por lo tanto el siguiente primo a probar multiplicado por los anteriores no podrá obtener el número como resultado, por lo que como mínimo obtendremos el número con el siguiente primo a probar por el mismo, esto significa que la búsqueda termina con el primo que tenga el cuadrado más cercano al número sin superarlo, o lo que es lo mismo:  
  
Para saber si un número es primo basta con probar si el número no es divisible por los primos hasta su raiz cuadrada.

CASO PRÁCTICO  
  
¿Es 149 primo?  
  
La raiz cuadrada de 149 es 12,2… por lo que solo es necesario probar los números primos hasta 12,2..  
  
probamos con 2,3,5,7,11  
  
149 : 2 = 74,5.. (no es divisible por 2)  
149 : 3 = 49,6.. (no es divisible por 3)  
149 : 5 = 29,8.. (no es divisible por 5)  
149 : 7 = 21,2.. (no es divisible por 7)  
149 : 11 = 13,5.. (no es divisible por 11)  
  
149 no puede ser dividido por estos primos por tanto 149 es un número primo.  
  
¿Existe una fórmula que me diga exactamente si un número es primo?  
  
Sí, el teorema de Wilson:  
  
Un número n es primo si y solo si (n-1)! + 1 es múltiplo de n  
  
Ejemplo:  
  
¿Es 7 primo?  
  
7 es primo si (7-1)! + 1 es múltiplo de 7  
  
(7-1)! + 1 = 6! + 1 = (6·5·4·3·2·1)+1 = 5040  
  
¿5040 es múltiplo de 7?  
  
5040 : 7 = 720 (división exacta)  
  
5040 sí es múltiplo de 7 por tanto 7 es un número primo.  
  
El problema viene cuando tenemos números mas grandes ya que el factorial se hace muy grande por lo que en definitiva no es un método práctico.  
  
Existen test mucho más complejos pero de difícil aplicación práctica si no es mediante programación en una computadora:  
  
PROBABILÍSTICOS  
  
Test de Solovay-Strassen (SS)  
Test de Miller-Rabin  
prueba de primalidad por curva elíptica  
DETERMINISTAS  
  
Test de Fermat (Solo primos de Mersenne)  
Test de Lucas-Lehmer (Solo primos de Mersenne)  
prueba por Pocklington  
Prueba LKL (Solo primos de Mersenne)  
En 2002 apareció un test determinista que asegura en un tiempo polinomial si un número es primo o no. Se conoce como el test AKS y es el descrubrimiento moderno en números primos más importante que se ha hecho.

<https://es.wikipedia.org/wiki/Test_de_primalidad_AKS>