Conjeturas acerca de la densidad de primos especiales

Raúl Durán Díaz

Departamento de Automática
Universidad de Alcalá de Henares
Ctra. Madrid-Barcelona km 33,600. 28871-Alcalá de Henares
raul.duran@uah.es

En este artículo abordamos el estudio de ciertas clases de primos cuyo uso resulta de interés en algunos criptosistemas de clave pública por estar dotados de propiedades especiales.

Se han considerado las siguientes clases de primos:

1. Los primos 1-seguros, determinados por la siguiente propiedad: un primo p se denomina 1-seguro si y sólo si $p = 2q + 1$, donde q es otro primo.

2. Los primos 2-seguros, determinados por la siguiente propiedad: un primo p se dice 2-seguro si $p = 2q + 1$ y además q es 1-seguro.

3. Los primos robustos[1]. Podemos decir que esta clase de primos presenta varias variantes, que comparten entre sí la propiedad de que si p es un primo robusto entonces $p+1$ y $p-1$ contienen factores primos "grandes"; y además algunos de estos factores presentan a su vez esta misma propiedad.

Hemos generalizado las definiciones de los puntos 1 y 2 introduciendo la noción de primo k-seguro de signatura arbitraria. Por ejemplo, de acuerdo con tal definición existen dos clases de primos 1-seguros: los de signatura $+1$, que coinciden con los definidos en el punto 1 anterior; y los de signatura -1, que se escriben como $p = 2q - 1$, donde q es otro primo.

También se ha introducido una clase novedosa de primos robustos que designamos como "primos robustos óptimos". La novedad consiste en definir una cierta función σ de variable discreta que permite caracterizar el grado de "robustez" de un primo robusto. Concretamente, los primos robustos óptimos son los mínimos de la función σ en el conjunto de los primos mayores o iguales que 23.

[1] Queremos proponer este término como equivalente para el mundo hispanohablante de lo que en la literatura anglosajona se conoce con el nombre de "strong primes".