The Numeric Field Sieve

Facultad de Ingeniería, Universidad de Cuenca
Abad L. Freddy., Aguilar Y. Bryan, Sigua L. Edisson.
Cuenca, Ecuador
{freddy.abadl, bryan.aguilar, edisson.sigua1407}@ucuenca.edu.ec

Abstract. -. La evolución que ha tomado la computación en la actualidad, se ha caracterizado por ser un crecimiento computacional exponencial. A pesar de ser muchas las ventajas que esto otorga, presenta complejos problemas a resolver. Así, se ha creado métodos de seguridad y el uso de la criptología para poder proteger los datos que circulan a través de la inmensa red que es el internet. Un gran exponente que se sigue utilizando hasta este momento es el cifrado RSA donde su fuerte en la dificultad computacional y matemática de factorizar números de muchos dígitos, pero al mismo tiempo se han ido inventando algoritmos para factorizar grandes números, donde los más utilizados son la criba cuadrática, y el motivo de este documento la criba de cuerpos numéricos.

Index Terms - *RSA, Sieve, Factorization;.*

I. INTRODUCCIÓN.

La revolución que produjo la Web y los constantes cambios que se generan diariamente, los avances en tecnologías tales como IoT genera diversas ventajas y conflictos. El caso de la ciberseguridad es uno de estos. Uno de los sistemas más utilizados para asegurar la información que recorre en Internet es RSA, que se basa en la dificultad para factorizar un número entero de muchos dígitos en sus componentes primos. Por lo que si se llegara a desarrollar un algoritmo eficiente para factorizar arbitrariamente grandes números en una cantidad de tiempo "razonable" entonces el valor de seguridad de RSA sería completamente nula. El desarrollo reciente más emocionante en el problema de factorización de enteros es el tamiz de campo numérico. ha tenido algunos éxitos espectaculares con enteros en ciertas formas especiales, en particular la factorización en 1990 del número de 155 dígitos decimales $2^{252}+1$. Para enteros duros arbitrarios, ahora parece amenazar el tamiz cuadrático como el algoritmo de elección. en este documento se describen el tamiz de campo numérico y las ideas detrás de él

II. MARCO TEÓRICO

A. CRIBA DE CUERPOS NUMÉRICOS

El algoritmo de criba de cuerpos numéricos general es el método más rápido conocido para factorizar grandes números donde generalmente se consideran grandes a más de 110 dígitos. La investigación y el desarrollo de este algoritmo en los últimos cinco años ha facilitado factorizaciones de enteros que alguna vez se especuló que requerían miles de años para realizarlos. Esto lo convierte en el mejor algoritmo para descifrar claves en RSA sistema de criptografía de clave pública, uno de los métodos más frecuentes para transmitir y recibir datos secretos. Si bien este método tiene muchas características inexploradas que merecen una investigación más profunda, la complejidad del algoritmo impide que casi nadie, excepto un experto, investigue su comportamiento.

Las ideas que condujeron al algoritmo de Criba de Cuerpos Numéricos esta motivadas por las mismas ideas que condujeron al desarrollo de la Criba Cuadrática a partir del método de Dixon. Como se esperaba, las nociones de una base de factores, números suaves y dependencia se utilizan en la criba de cuerpos numéricos, junto con una perspectiva para encontrar números suaves que admitan un procedimiento de cribado. Un gran avance se produce al darse cuenta de que los polinomios cuadráticos del método de Dixon y de la criba cuadrática no necesariamente tienen que ser cuadráticos. Tal vez ciertos polinomios de grado cúbico, cuártico, quístico o incluso más alto podrían producir números más suaves que los cuadráticos.

1. Números suaves

Un entero n se dice $B-suave$, si todos los primos en su factorización son menores o iguales a B.

2. Base de Factores

El conjunto de primos menores que B (o a veces el conjunto de potencias de primos menores que B) es denominado base de factorización.

3. Proceso de Factorización

El primer paso para factorizar un número N mediante la criba general del cuerpo de números consiste en encontrar un polinomio $f(x)$ que sea irreducible en $Z[x]$ y que además tenga una raíz m módulo N. Para construir un polinomio en $Z_N[x]$ con una raíz m podemos hacerlo expresando el número N en $base-m$, es decir, expresamos N de la forma

$$N=\sum_{k=0}^{r} a_k m^k$$

y tomamos el polinomio

$$f(x)=\sum_{k=0}^{r} a_k x^k$$

de este modo ya tenemos un polinomio que cumpla con los requisitos.

Los polinomios candidatos a ser utilizados en el algoritmo son muchos y no existe un método para determinar cuál será el que mejor funciona al aplicar la criba general del cuerpo de números a cada número N. El siguiente paso consiste en determinar el dominio sobre el que sea va a aplicar el algoritmo. Para ello debemos especificar las distintas bases de factores que vamos a utilizar. Necesitaremos tres bases de factores: la base del factor racional, la base del factor algebraico y la base del carácter cuadrático.

La base del factor racional contendrá los números primos menores que un número ω que representará la cota de la base. No obstante, la base del factor racional no almacenará sólo dicha información, ya que cada número primo p se guardará junto al valor $p\ (mod\ m)$.

Por otro lado, la base del factor algebraico contendrá una lista con los pares (p, r) donde los números p son números primos y r es el menor número entero tal que $f(r) \equiv 0\ mod(p)$. El tamaño de la base del factor algebraico debe ser superior al de la base del factor racional.

Por último la base del carácter cuadrático tendrá una continuación de la base del factor algebraico, es decir, pares de números primos y las raíces pero con unos cuantos números p mayores que los anteriores. El tamaño de esta base de factores será inferior al de las anteriores.

El siguiente paso consiste en realizar una criba. Este es el cuello de botella del algoritmo ya que realiza operaciones muy costosas en términos computacionales sobre dominios muy grandes, por lo tanto la mayor parte del tiempo del algoritmo se invierte en este paso.

El proceso de criba persigue el objetivo de encontrar pares de números (a, b) que cumplan

- $mcd\,(a, b) = 1$
- $a + bm$ tiene todos sus factores en la base del factor racional.
- $(-b)^d f(a/b)$ tiene todos sus factores en la base del factor algebraico.

Para ello, tomaremos b fijo y variamos a en un intervalo $[-C, C]$ cuyo tamaño dependerá directamente del tamaño del número a factorizar. Si el valor escogido para C no es suficientemente grande, deberemos tomar un número C superior. De esta forma calcularemos para los pares (a, b) los factores de $a + bm$ y de aquellos que factorizan en la base del factor racional, nos quedaremos con aquellos para los que $(-b)^d f(a/b)$ tenga los factores en la base del factor algebraico.

Una vez hemos obtenido una lista de pares (a, b) que cumplen las propiedades requeridas, el objetivo es encontrar un subconjunto de la lista cuyo producto sea un número cuadrado. Nuevamente no necesitamos encontrar en la lista números cuadrados, nos basta con que el producto de varios de ellos sea un número cuadrado. Este paso se puede llevar a cabo resolviendo un sistema de ecuaciones lineales, ya que incluso para matrices de un tamaño elevado, el sistema sólo contendrá un 1 en las posiciones de los números primos que aparezcan como factor con potencia impar y un 0 en las posiciones de los números primos que aparezcan como un factor con potencia para o no aparezcan como un factor, se podrá resolver de un modo relativamente eficiente.

Una vez se obtiene una solución al sistema, es decir, cuando tenemos números $x\,e\,y$ cuyos cuadrados son congruentes módulo N, se produce como en el resto de algoritmos calculando $mcd(x - y, N)$ y $mcd\,(x + y, N)$ para ver si obtenemos un factor no trivial de N.

III. CONCLUSIONES.

La seguridad no se ha vuelto algo opcional para el momento en que vivimos se ha vuelto una necesidad, donde la criptografía tiene un gran protagonismo, pero al mismo tiempo que esta va aportando con nuevas técnicas, se debe adaptar a la evolución computacional que están comenzando a tener la potencia computacional para poder romper los métodos criptográficos.

La criba de cuerpos numéricos se ha convertido en la actualidad el algoritmo más rápido para factorizar números de más de 100 dígitos. Esto lo convierte en el mejor algoritmo para descifrar claves en RSA sistema de criptografía de clave pública, uno de los métodos más frecuentes para transmitir y recibir datos secretos.

Existe una correlación entre los desarrollos algorítmicos y la evolución del hardware de la computadora. Aunque Lehmer y Power-s en 1931 tenían casi todos los ingredientes del algoritmo de factorización de fracción continua, no dieron el salto a números lisos y los vectores de exponentes reducidos. Módulo 2 lo hicieron Brillhart y Morrison, casi seguramente porque estas ideas no son muy adecuadas Para los cálculos de mano que hicieron Lehmer y Powers. De manera similar, Kraitchik, 50 años antes de la introducción del tamiz cuadrático, había sugerido encontrar un conjunto de números enteros τ con $\Pi_{t\varepsilon\tau}\,(t^2 - n)$ un cuadrado como una forma de factorizar n. Debido a que no tenía una computadora grande para trabajar, no se le ocurrió la idea de tamizar para descubrir valores suaves de $(t^2 - n)$ y luego combinarlos a través del álgebra lineal $mod\ 2$.

En cierto sentido, el tamiz de campo numérico para enteros generales puede estar un poco adelantado a su tiempo. Aunque heurísticamente es el campeón asintótico, aún no ha factorizado el número compuesto más grande De ninguna forma especial y sin factor primo pequeño nunca factorizado. Este honor aún pertenece al tamiz cuadrático. Creemos que estamos cerca del punto de cruce ahora, es decir, de 120 a 130 dígitos decimales. Pero para tener en cuenta estos números se necesita una enorme cantidad de potencia de cálculo, a pesar de nuestros algoritmos inteligentes. Tal vez dado un mejor orden de magnitud de la velocidad (y el tamaño) de las computadoras, creo que el tamiz de campo numérico surgirá como el método claro de elección para los números más difíciles.

IV. REFERENCIAS BIBLIOGRÁFICA

[1] Urko Nalda Gil, "Factorización". Universidad de la Rioja (2014). Retrieved from: https://biblioteca.unirioja.es/tfe_e/TFE000668.pdf [Accessed 1 Jul. 2019].

[2] Aylen Martnez Lopez & Martn Mara, "Una breve introducción a la criptografía matemática - PDF". (2015). Retrieved from: https://docplayer.es/51519095-Una-breve-introduccion-a-la-criptografia-matematica.html [Accessed 1 Jul. 2019].

[3] Carl Pomerance, "Numeric Field Sieve" American Mathematical Society (1994). Retrieved from: https://www.math.dartmouth.edu/~carlp/PDF/paper99.pdf [Accessed 1 Jul. 2019].

[4] L.M. Adleman, "Factoring numbers using singular integers". (1991). Retrieved from: https://www.ams.org/journals/mcom/2003-72-242/S0025-5718-02-01482-5/ [Accessed 1 Jul. 2019].

Análisis de la Hipótesis de Riemann

Abad L. Freddy., Aguilar Y. Bryan, Sigua L. Edisson.
Facultad de Ingeniería, Universidad de Cuenca
Cuenca, Ecuador
{freddy.abadl, bryan.aguilar, edisson.sigua1407}@ucuenca.edu.ec

Abstract — *Casi todos los matemáticos del mundo afirman que el problema más importante de las matemáticas es la hipótesis de Riemann. Este problema fue uno de los 23 problemas de la lista de Hilbert que influyó en las matemáticas del siglo XX; es uno de los problemas del milenio que aún sigue sin resolverse. Desde 1859 cuando Riemann efectuó su trabajo matemático, encontrando una aproximación a la estimación de la cantidad de primos menores o iguales a un valor x, conjeturando que todos los ceros no triviales de la función que desarrollo se encuentran en $S = \frac{1}{2} + ti$ donde $S \in \mathbb{C}$ y $t \in R$, de ahí que los matemáticos han buscado poder demostrar su hipótesis.*

Index Terms — Función Zeta, números primos,.

.

I. Introducción

Desde Euclides (año 300 a. C.) se sabe que la sucesión de números primos es infinita. En 1737 Euler demostró que $\Sigma_n \frac{1}{p_n}$ diverge, lo cual conduce a otra demostración de la existencia de infinitos números primos. Uno de los más notables descubrimientos de Euler fué $\Sigma_{n=1}^{\infty} n^{-2} = \frac{\pi^2}{6}$. La observación de Euler de que el producto:

$$\prod_p \{1 - p^{-s}\}^{-1} = \sum_{n=1}^{\infty} n^{-s}, \quad s > 1$$

Fig. 1. Observación del producto de Euler (1749)

donde p recorre todos los números primos p y n los naturales, marcó el inicio de las investigaciones de Riemann.

El interés de la localización de los ceros de la función zeta de Riemann fue destacado por el matemático alemán David Hilbert, en 1900, en el problema octavo de su lista de veintitrés problemas abiertos que presentó en el Congreso Internacional de Matemáticos, celebrado en París al inicio del pasado siglo. En el decurso de los años, se ha ido poniendo de relieve que la función zeta interviene en muchos problemas aritméticos, por lo que una demostración de la hipótesis de Riemann confirma la validez de gran cantidad de resultados numéricos que dependen de esta afirmación. En particular, la función zeta es, de lejos, la herramienta analítica más importante para estudiar los números primos.

II. Inicios de la investigación de Riemann

Resulta difícil ver cómo la representación de un producto (Fig. 1.) puede ayudar a establecer un planteamiento analítico para la función $\pi(x)$, esto se refiere a la cantidad de números primos en el intervalo $[1, x]$. La distribución de los números primos es realmente incomprensible. Riemann se planteó cuestiones como: la distribución de los números primos, la existencia de infinitos números primos, determinar fórmulas que permitan obtener esos números primos, la medida de intervalos entre números primos, etc.

Legendre y Gauss se interesaron por el problema de establecer la cantidad de números primos que hay en un intervalo $[1, x]$. Legendre afirmaba que para valores suficientemente grandes $\pi(x)$ es aproximadamente $\frac{x}{(\log x - 1.08366)}$. Por otra parte Gauss, calculando la cantidad de números primos consecutivos que hay en cada mil números de la sucesión natural, afirmaba que $\pi(x)$ se asemeja a la integral $li(x) = \int_2^x \frac{dt}{\log t}$. Estas hipótesis (Legendre y Gauss) se expresan con las fórmulas:

$$\pi(x) \approx \frac{x}{\log x}, \qquad \pi(x) \approx \int_2^x \frac{dt}{\log t}.$$

Fig. 2. Fórmulas de hipótesis de Legendre y Gauss.

Con una integración por partes se puede demostrar

$$li\, x = \int_2^x \frac{dt}{\log t} = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{dt}{\log^2 t} \sim \frac{x}{\log x}$$

Fig. 3. Equivalencia entre hipótesis de Legendre y Gauss

De modo que $\pi(x) \sim li$ y $\pi(x) \sim \frac{x}{\log x}$, cuando $x \to \infty$ son equivalentes. Gauss conjeturó que la funciones $li(x)$ y $\pi(x)$ están muy cerca la una de la otra, y que la probabilidad de que un número grande y arbitrario x sea primo está cerca de $\frac{1}{\log x}$.

La equivalencia asintótica denotada por $\pi(x) \sim \frac{x}{\log x}$, cuando $x \to \infty$. Es la que se conoce como el teorema de los números primos. La existencia del límite la demostraron Hadamard y de la Vallée Poussin en 1896, mediante las ideas desarrolladas por Riemann relacionadas con la función ζ(s) para valores complejos de s.

III. Desarrollo de la función $F(x)$ realizada por Riemann

Aunque Riemann, no logró demostrar el teorema de los números primos (demostrado por Hadamard y de la Vallée Poussin en 1896). Riemann hizo mucho más que dar una aproximación $F(x)$ a $\pi(x)$ más precisa que la $li(x)$ de

Gauss: consiguió dar una fórmula exacta para $\pi(x)$. Concretamente, Riemann estudió con precisión el error:

$$E(x) = \pi(x) - li(x)$$

Riemann, alumno de Gauss, consideró la posibilidad de describir con precisión el término de error $E(x)$. El estudio que para ello llevó a cabo de la distribución de los números primos, le llevó a sugerir una nueva función para aproximar $\pi(x)$, al observar que la probabilidad de que un número grande x elegido al azar sea primo es aún más cercana a $\frac{x}{\log x}$ si se considera no sólo los primos, sino también las potencias de los primos, contando el cuadrado de un primo como medio primo, la potencia cúbica como un tercio de primo, etc., esto es

$$\pi(x) + \frac{1}{2}\, Li(x^{\frac{1}{2}}) + \frac{1}{3}\, Li(x^{\frac{1}{3}}) + \frac{1}{5}\, Li(x^{\frac{1}{5}}) - \frac{1}{6}\, Li(x^{\frac{1}{6}}) - \frac{1}{7}\, Li(x^{\frac{1}{7}}) \ldots = Li(x)$$

Fig. 4. Sucesión de potencias de primos

O de manera equivalente $\pi(x) \approx R(x)$ donde $R(x)$ se define como:

$$R(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n}\, Li(x^{\frac{1}{n}})$$

Fig. 5. Definición de la aproximación de $\pi(x)$

Donde $\mu(n)$ es la función de Möbius, que toma el valor 0 si n es divisible por el cuadrado de algún primo, 1 si n es el producto de un número par de primos distintos y -1 si n es un producto de una cantidad impar de primos. Esta función $R(x)$ representa una aproximación sorprendentemente buena a $\pi(x)$. Ver Fig. 6.

x	$\pi(x)$	$R(x)$
100.000.000	5.761.455	5.761.552
200.000.000	11.078.937	11.079.090
300.000.000	16.252.325	16.252.355
400.000.000	21.336.326	21.336.185
500.000.000	26.355.867	26.355.517
600.000.000	31.324.703	31.324.622
700.000.000	36.252.931	36.252.719
800.000.000	41.146.179	41.146.248
900.000.000	46.009.215	46.009.949

Fig. 6. Aproximación de $\pi(x) \approx R(x)$

Más allá de dar una aproximación de $\pi(x)$ *a* $R(x)$ Riemann estudió con precisión el error

$$\pi(x) - R(x)$$

Y logró construir una serie infinita de términos correctores $C_1(x), C_2(x), \ldots R(x)$ de tal manera que

$$R_k(x) = R(x) + C_1(x) + C_2(x) + \ldots + C_k(x)$$

Verifican $\lim_{k\to\infty} R_k(x) = \pi(x)$. Riemann empleó la función zeta de Euler definida por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}$$

Fig. 7. Función zeta de Euler

Para construir términos correctores, las funciones zeta aparecen como series o productos infinitos que permiten organizar colecciones de datos numéricos de forma única y compacta. Euler fue el primero que introdujo este tipo de funciones para estudiar los números primos. Euler había estudiado esta función real de variable real

$$\zeta : \mathbf{R} \to \mathbf{R} \cup \{\infty\}$$

$$s \to \zeta(s),$$

Fig. 8. Función real zeta de variable real

que verifica que si $s > 1$, $\zeta(s) < \infty$, e intentó utilizar esta función para estudiar los números primos. Sin embargo, considerada como una función real de variable real se trata de un objeto unidimensional, no tiene suficiente estructura geométrica como para poder desvelar (o codificar) el patrón de distribución de los números primos.

IV. Extensión de Riemann de valores reales a complejos

Riemann dio un gran salto al extender $\zeta(s)$ a valores complejos de la variable $s \neq 1, s = a + bi$ donde $i = \sqrt{-1}$ y $a, b \in R$. Riemann considero

$$\zeta : \mathbb{C} \setminus \{1\} \to \mathbb{C}$$

$$s \to \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Es decir, la función zeta de Riemann o función Euler-Riemann es una función de una variable compleja que analíticamente continua la suma de la serie de Dirichlet. En matemáticas, una serie de Dirichlet es toda serie de tipo

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

donde s y a_n para n = 1, 2, 3, ... son números complejos. Las series de Dirichlet juegan un papel importante en la teoría analítica de números. **La definición más popularizada de la función zeta de Riemann es una serie Dirichlet**.

La serie converge para todos los números complejos con la parte real y para este caso se define $\zeta(s)$:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

Y se define por la integral

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{x^{s-1}}{e^x - 1} dx$$

Donde $\Gamma(s)$ es la función Gamma. Dicho de otra manera se puede definir la función zeta de Riemann como:

"La extensión analítica a todos los complejos de la función $\zeta(s)$ que está definida para los complejos cuya parte real es mayor que 1"

V. Hipótesis de Riemann

Como se mencionó en la sección anterior, las cuestiones relacionadas a los números primos está relacionada con las propiedades de la función.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Riemann construyó un paisaje matemático como una gráfica tridimensional y descubrió que los puntos que se encontraban a lo equivalente al nivel del mar "puntos cero" eran los que esconden los secretos de los números primos. Ver Fig. 3.

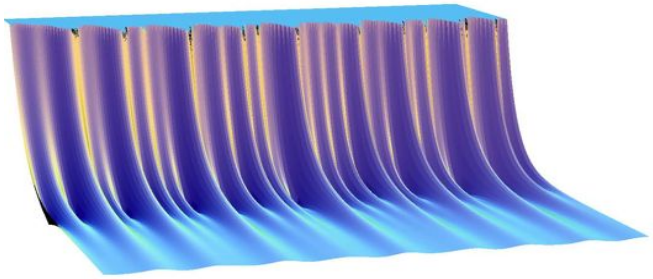

Fig. 9. Paisaje matemático ideado por Riemann

Según Riemann la ubicación de aquellos ceros implicaba que la naturaleza distribuía los números primos equitativamente por todo el universo de los números. Y asumió que todos los ceros, por infinitos que fueran se encontraban en la misma línea recta.

A. Ceros de la función $\zeta(s)$ de Riemann

Con respecto a los ceros de la función $\zeta(s)$ se consideran tres aspectos: a) el número de ceros que hay en un rectángulo de la franja cr´ıtica, b) la magnitud de los intervalos entre ceros consecutivos de la línea crítica y c) la obtención de regiones de la franja crítica donde $\zeta(s) \neq 0$.

Si $\zeta(s) > 1$, la existencia del producto de Euler garantiza que $\zeta(s) \neq 0$, pues el producto converge y toma valores no nulos. Riemann sabía que en esta franja vertical (donde se encuentran los ceros de la función), llamada franja crítica, hay una infinidad de ceros de $\zeta(s)$. En 1889 Riemann había conseguido calcular la primera docena de los ceros de la función zeta en la franja crítica, y había descubierto que todos ellos tenían como parte real 1/2.

En una memoria de 1859, Riemann comentó que este podría muy bien tratarse de un hecho general, aunque él no sabía cómo justificarlo. La hipótesis de Riemann presupone que todos los ceros no triviales de la función zeta se sitúan en la recta x=1/2, denominada «recta crítica».

La Figura 10 representa las curvas de nivel de los ceros de las partes real (en rojo) e imaginaria (en azul) de $\zeta(s)$. Los ceros, representados por un punto negro, se encuentran donde las dos curvas se cortan. Se pueden ver los dos primeros ceros triviales y los diez primeros ceros no triviales y sus simétricos, todos estos sobre la recta crítica.

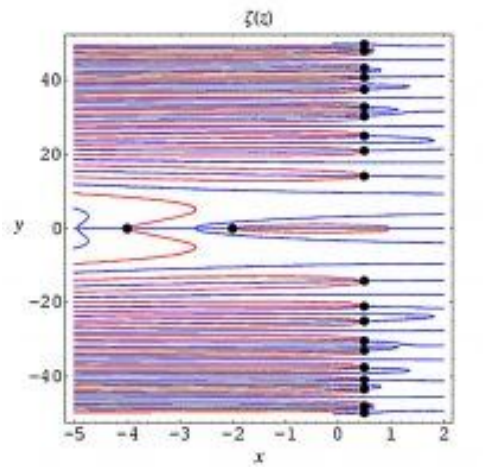

Fig. 10. Primeros ceros de la función zeta de Riemann.

VI. Algunas peculiaridades de la hipótesis de Riemann

Muchos definen la hipótesis de Riemann de diferentes maneras, sin embargo, una buena definición para dicha hipótesis es:

"*La parte real de todos los ceros no triviales de la función zeta de Riemann es* $\frac{1}{2}$"

Como se ha mencionado en secciones anteriores, la función zeta de Riemann es la extensión analítica a todos los complejos de la función

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

que está definida para los complejos cuya parte real es mayor que 1. Riemann consideró puntos en los que la función zeta se hace cero, la primera observación que dió es que todos los números pares negativos son lugares donde dicha función se hace cero. Esto debido a que la función zeta satisface la siguiente ecuación funcional

$$\zeta(z) = 2^z \pi^{z-1} \sin(\pi z/2) \Gamma(1-z) \zeta(1-z)$$

Fig. 11. Ecuación funcional de Riemann

Se puede demostrar que todos los ceros de la función zeta son complejos cuya parte real está entre 0 y 1, a esa franja se

la denomina *franja crítica* y en medio de dicha región crítica está la línea crítica (Ver Fig. 12) que es la línea de los números complejos cuya parte real es $\frac{1}{2}$ y la hipótesis de Riemann afirma que todos los ceros no triviales se encuentran en dicha línea.

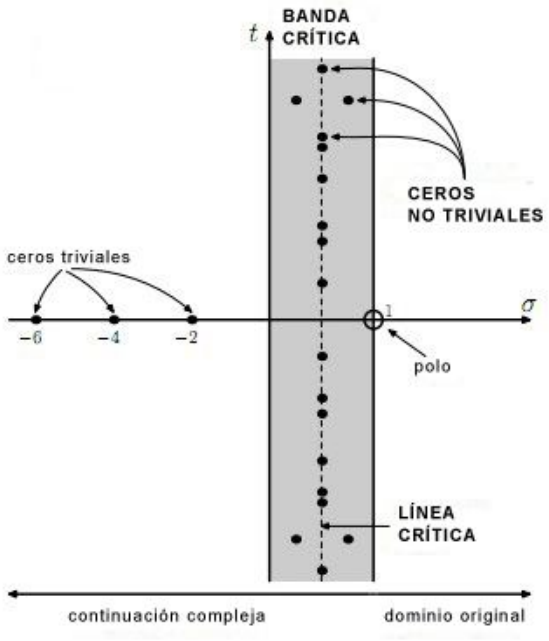

Fig. 12. Región y línea crítica de la función zeta de Riemann

De estos ceros en la línea crítica se sabe que:

- Existen infinitos ceros en la línea crítica, este enunciado fue demostrado por el matemático Godfrey Hardy.
- Desde el año 1989 se sabe que al menos ⅖ de todos los ceros están en la línea crítica.
- Se sabe que los ceros de la función zeta están bastante unidos a la línea crítica, se ha demostrado dado un número infinitesimal denotado como épsilon ε, se sabe que todos los ceros, salvo una porción mínima están a una distancia menor que epsilon de la línea crítica.
- Algunos matemáticos famosos han calculado ceros de la función zeta de Riemann, por ejemplo Alan Turing calculó más de mil.
- En la actualidad, se conocen muchos ceros de la función zeta de Riemann (billones y billones de ceros de dicha función), todos y cada uno de ellos se encuentran en la línea crítica.

VII. Conclusiones

La hipótesis de Riemann afirma que todos los ceros no triviales de la función zeta se encuentran en la recta $x = \frac{1}{2}$. Más de diez billones de ceros calculados hasta hoy, todos alineados sobre la recta crítica, corroboran la sospecha de Riemann, pero nadie aún ha podido probar que la función zeta no tenga ceros no triviales fuera de esta recta.

Muchos algoritmos para construir primos grandes que funcionan de manera muy eficiente están construidos sobre la base de que la conjetura de Riemann es cierta, algo que se da por hecho en prácticamente toda la comunidad matemática.

En particular, la función zeta es, de lejos, la herramienta analítica más importante para estudiar los números primos. Más de diez billones de ceros de la función zeta calculados hasta hoy con la ayuda de los ordenadores, todos alineados en la recta crítica, hacen patente la extraordinaria intuición de Riemann.

VIII. Referencias

[1] Bayer, P. (2017). LA HIPÓTESIS DE RIEMANN EL GRAN RETO PENDIENTE. 1st ed. [ebook] Valencia, pp.1-7. Available at: https://metode.cat/wp-content/uploads/2017/06/93ES-MONO-2-hipotesis-riemann.pdf [Accessed 1 Jul. 2019].

[2] Calderón, C. (2002). La Función Zeta de Riemann. 1st ed. [ebook] Zaragoza, pp.67-87. Available at: http://www.raczar.es/webracz/ImageServlet?mod=publicaciones&subMod=revistas&car=revista57&archivo=067.pdf [Accessed 2 Jul. 2019].

[3] Corrales, C. (n.d.). NÚMEROS EN NÚMEROS. 1st ed. [ebook] pp.1-14. Available at: https://dialnet.unirioja.es/servlet/articulo?codigo=2529618 [Accessed 1 Jul. 2019].

[4] Porras, J. (2017). ANÁLISIS DE LA HIPÓTESIS DE RIEMANN. 1st ed. [ebook] Cartajena, pp.2-34. Available at: https://www.researchgate.net/publication/315844833_ANALISIS_DE_LA_HIPOTESIS_DE_RIEMANN [Accessed 1 Jul. 2019].