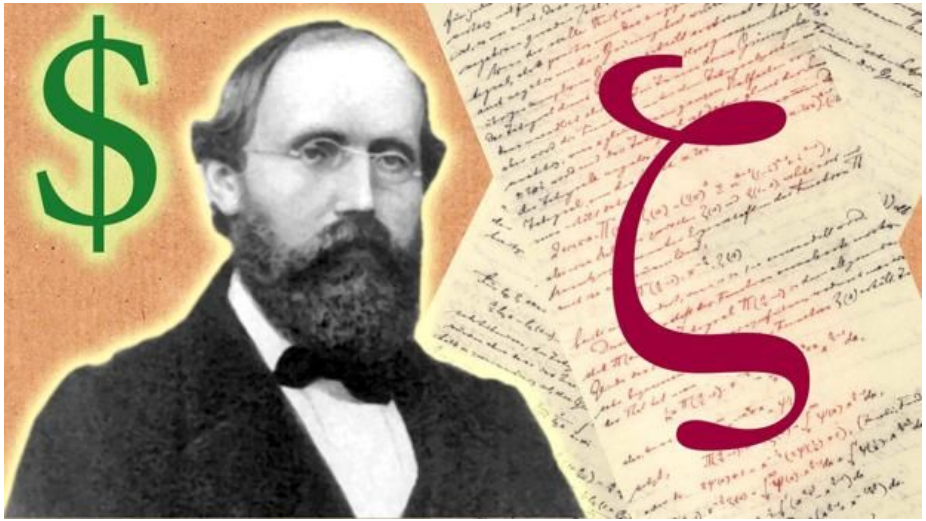
Hipótesis de Riemann
Criba de Cuerpo Numérico

Abad Freddy
Aguilar Bryan
Sigua Edisson

Optativa 4 - Criptología

Análisis de la Hipótesis de Riemann



Introducción

- Matemáticos afirman que se trata del problema más importante de las matemáticas.
- Este problema fue uno de los 23 problemas de la lista de Hilbert que influyó en las matemáticas del siglo XX.
- 1859. 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:

$$S = 1/2+ti \text{ donde } S \in C \text{ y } t \in R.$$

Orígenes de la hipótesis de Riemann

- 300 aC: Desde Euclides, se sabe que la sucesión de números primos infinita.
- 1737: Euler demostró que $\sum_n 1/p_n$ diverge → demostración de infinitos primos
- Notables descubrimientos de Euler

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

donde p recorre todos los números primos p y n los naturales.

- Marcó el inicio de las investigaciones de Riemann

Orígenes de la hipótesis de Riemann

- Representación de un producto ayudar a establecer planteamiento analítico para π(x) → cantidad de primos en el intervalo [1,x]
- Riemann → cuestiones: distribución de primos, existencia de infinitos primos, fórmulas para obtener primos, 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]. Establecieron hipótesis:
- Además

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

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

Orígenes de la hipótesis de Riemann

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

- Se sabe que:

$$\pi(x) \sim li\ x \text{ y } \pi(x) \sim \frac{x}{\log x}, x \to \infty$$

- Gauss conjeturó que li(x)y (x) están muy cerca. Probabilidad de que un número grande y arbitrario x sea primo está cerca de x/log x
- La equivalencia asintótica denotada por $\frac{x}{\log x}, x \to \infty$ Es la que se conoce como el teorema de los números primos.

Función zeta de Riemann

- Al verificar que:

$$\lim_{k\to\infty} R_k(x) = \pi(x)$$

- Riemann empleó la función zeta de Euler definida por

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

- Funciones zeta: series o productos infinitos que permiten organizar colecciones de datos numéricos. Euler introdujo estas funciones para estudiar los números primos. Euler había estudiado esta función real de variable real.

Función zeta de Riemann

- Considerar variable real, Euler, se dio cuenta que no tiene suficiente estructura geométrica como para codificar la distribución de números primos.
- Riemann dio un gran salto al extender ζ(s) a valores complejos de la variable s≠1, s=a+bi donde i=√-1 donde a, b ∈ R.
- La función zeta de Riemann o función Euler-Riemann es una función de variable compleja que es analíticamente continua.
- La serie converge para todos los números complejos con la parte real y para este caso se define ζ(s):

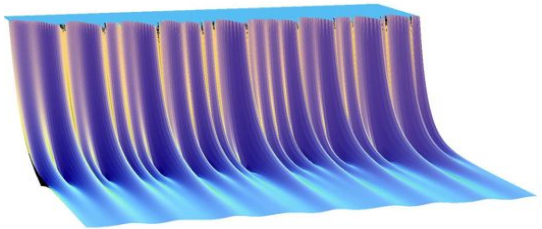
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

“Es la extensión analítica a todos los complejos de la función ζ(s) que está definida para los complejos cuya parte real es mayor que 1”

Definición de la función zeta de Riemann

Hipótesis de Riemann

- 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.



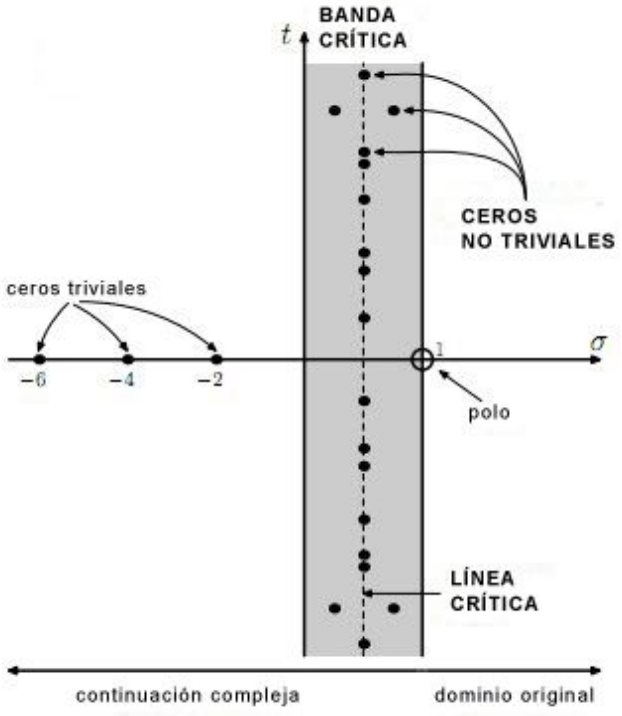
- La ubicación de los ceros implica la distribución de los primos en el universo de los números. Asumió que todos los ceros, por infinitos que fueran se encontraban en la misma línea recta.

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».
- Muchos definen la hipótesis de Riemann de diferentes maneras, una buena definición para dicha hipótesis es:

  “La parte real de todos los ceros no triviales de la función zeta de es 12”

- Observación Riemann: pares negativos son lugares donde la función es 0.



Aspectos importantes

- Existen infinitos ceros en la línea crítica, este enunciado fue demostrado por el matemático Godfrey Hardy.
- Desde 1989 se sabe que al menos ⅖ de todos los ceros están en la línea crítica.
- 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.

Análisis de la Criba de Cuerpo Numérico

363	424	646	747	757	767	787	393
696	232	383	898	939	969	242	525
676	949	222	595	737	888	272	545
656	868	959	666	444	373	353	565
636	343	484	333	999	626	878	585
535	292	777	848	262	555	929	686
494	979	838	323	282	252	989	727
828	797	575	474	464	454	434	858

Introducción

- Método más rápido conocido para factorizar números grandes de más de 110 dígitos.
- Basado en la Criba Cuadrática a partir del método de Dixon (nociones de una base de factores, números suaves y dependencia se utilizan en la criba de cuerpos numéricos).
- 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 2252+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

Base Matemática

- Para factorizar un número *N* con la criba de cuerpo numérico se debe encontrar una función *f(x)* irreducible en *Z[x]* y que además tenga una raíz *m* módulo *N*.
- Para construir un polinomio en Z[x] con una raíz *m* debe expresar el número *N* en *base-m*, es decir, expresamos *N* de la forma

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

- Tomando el polinomio

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

Base Matemática

- Determinar el dominio sobre el que se va a aplicar el algoritmo especificando las bases de factores a utilizar:
  - Base del factor racional.
  - Base del factor algebraico
  - Base del carácter cuadrático.

Base del Factor Racional

- Contiene los números primos menores que un número ***w*** que representará la cota de la base.
- La base del factor racional también almacenará cada número primo ***p*** junto al valor *p (mod m)*.

Base del Factor Algebraico

- Contiene 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) = 0 mod(p)***.
- El tamaño de la base del factor algebraico debe ser superior al de la base del factor racional.

Base del Factor Cuadrático

- Contendrá 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.

Proceso de Cribado

- 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.

Proceso de Cribado

- Escoger un ***b*** fijo y variar ***a*** en un intervalo ***[-C, C]*** cuyo tamaño dependerá directamente del tamaño del número a factorizar. El tamaño escogido para ***C*** debe ser lo suficientemente grande.
- Calcular los pares ***(a, b)*** para los factores de ***a+bm*** y de aquellos que factorizan en la base del factor racional.
- Mantenemos aquellos para los que ***(-b)^d * f(a/b)*** tenga los factores en la base del factor algebraico.
- Obtenida la 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**.

Proceso de Cribado

- Escoger un número cuadrado se puede llevar a cabo resolviendo un sistema de ecuaciones lineales.
- 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.
- 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***.