# Consecuencias de la Hipótesis de Riemann

Este artículo se basa en la traducción de la respuesta de K. Conrad a la pregunta formulada más abajo y que apareció en mathoverflow.net (sitio de preguntas y respuestas para matemáticos). Cabe destacar que la lista de resultados presentados se caracterizan por ser consecuencia de la Hipótesis de Riemann (RH) o la Hipótesis de Riemann Generalizada (GRH), pero en la mayoria de los casos se han obtenido posteriormente demostraciones de estos mismos resultados sin usar estas hipótesis. El autor remarca que es como si la RH condujera a la respuesta correcta.

**Pregunta**: Supongo que una serie de resultados han sido demostrados como consecuencia de la Hipótesis de Riemann (RH), por supuesto, en el área de teoría de números y también en otros campos. ¿Cuáles son los resultados más relevantes que se cononcen? También sería interesante incluir consecuencias de la hipótesis de Riemann generalizada (GRH) (pero especificado cuál de las dos se supone en cada caso).

**Nota** La lectura de esta nota requiere conceptos matemáticos, quizás ajenos a algunos lectores. Sugerimos a los lectores versados a redactar apéndices que expliciten lo resumido en esta nota.

Para entender la respuesta, repasemos algunos conceptos. La función zeta de Riemann, es una función holomorfa en $\mathbb{C}\backslash\{1\}$, que posee ceros en los números

$$\{0, -2, -4, -6, \dots\}.$$

La Hipótesis de Riemann (RH)[1] afirma que todos los otros ceros de la función zeta se encuentran en la recta vertical que pasa por $\frac{1}{2}$. Esto es, son números complejos de la forma $\frac{1}{2} + it$, $t$ un número real apropiado.

La función zeta esta definida para números complejos $s = a + ib$ con $a > 1$ por el límite de la sucesión

$$z(s) = \lim_{k\to\infty}(1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots + \frac{1}{k^s}).$$

En otra notación

$$z(s) = \sum_{k=1}^{\infty} \frac{1}{k^s} = \prod_{p\, primo} \frac{1}{(1 - p^{-s})}.$$

Se demuestra que la funcón zeta se extiende a una función holomorfa en $\mathbb{C}\backslash\{1\}$.

[1] Enunciada por Riemann aproximadamente en 1850

Hoy día sabemos que $z(3)$ es un número irracional, pero no sabemos cual de los números

$$z(5), z(7), z(9), \ldots$$

es racional o irracional.

Si sabemos que para $k$ un número natural mayor o igual a uno, vale

$$z(2k) = (-1)^{k+1} \frac{B_{2k}(2\pi)^{2k}}{2(2n)!}$$

donde $B_{2k}$ es el número de Bernoulli. $B_{2k}$ es un número racional!

El estudio de la distribución de los números primos es uno de los problemas abiertos más importantes en la matemática contemporánea. La función zeta de Riemann tiene una profunda conexión con los números primos. La formulación tradicional de la hipótesis de Riemann oscurece un poco la importancia real de la conjetura. Para comenzar con un ejemplo, más bien vago, puntualizamos:

Los ceros de la función zeta y los números primos satisfacen ciertas propiedades de dualidad, conocidas como fórmulas explícitas, que muestran, usando análisis de Fourier, que los ceros de la función zeta de Riemann pueden interpretarse como frecuencias armónicas en la distribución de los números primos.

La hipótesis generalizada de Riemann (GRH)(para las funciones-L de Dirichlet) fue probablemente enunciada por primera vez por Piltz en 1884. Al igual que la hipótesis original de Riemann, posee consecuencias que abarcan a la distribución de los números primos.

El enunciado formal de la GRH es el siguiente. Un carácter de Dirichlet es una función aritmética ($\chi : \mathbb{Z} \to \mathbb{Z}$) completamente multiplicativa tal que existe un entero positivo $k$ con $\chi(n + k) = \chi(n)$ para todo $n$ y $\chi(n) = 0$ siempre que m.c.d$(n, k) > 1$. Si tal carácter existe, se define la función-L de Dirichlet correspondiente mediante

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

para todo número complejo $s$ con parte real mayor que 1. Por extensión analítica, esta función puede ser extendida a una función meromorfa definida sobre todo el plano complejo. La Hipótesis generalizada de Riemann establece que para todo carácter de Dirichlet $\chi$ y todo número complejo $s$ con $L(\chi, s) = 0$, si la parte real de $s$ se encuentra comprendida entre 0 y 1, entonces es igual a 1/2. El caso $\chi(n) = 1$ para todo $n$ conduce a la Hipótesis de Riemann (RH).

A continuación presentamos la respuesta de K. Conrad sobre consecuencias de la RH.

**Respuesta de K. Conrad:** Di una charla sobre este tema hace unos meses, y redacté una lista de consecuencias de la RH que podría ser adecuada para un público matemático general.

Vamos a empezar con tres aplicaciones de RH para la función zeta de Riemann solamente.

1. *Estimadores precisos del término del resto del teorema de los números primos:* Hege von Koch demostró en 1901 que la hipótesis de Riemann es equivalente al considerable refinamiento del teorema de los números primos.
   Existe una constante $C > 0$ tal que

   $$|\pi(x) - Li(x)| \leq C\sqrt{x}\,\ln(x),$$

   para todo $x$ suficientemente grande, donde

   $$\pi(x) = card\{p \geq 2, \text{primo}, p \leq x\}$$

   es la función contadora de primos y $Li(x) = \int_2^x \ln(t)\,dt$ con $\ln(x)$ el logaritmo natural de $x$.

2. *Comparación de $\pi(x)$ y $Li(x)$.* Para valores de $x$ pequeños se había demostrado que $\pi(x) < \mathrm{Li}(x)$ lo que llevó a conjeturar a varios matemáticos en la época de Gauss que $\mathrm{Li}(x)$ era una cota superior estricta de $\pi(x)$ (esto es que la ecuación $\pi(x) - \mathrm{Li}(x) = 0$ no tiene soluciones reales). Pero en 1914 Littlewood utilizó la Hipótesis de Riemann para mostrar que la desigualdad $\pi(x) < Li(x)$ se invierte para valores suficientemente grandes de $x$. En 1933, Skewes utilizó la RH para mostrar que la desigualdad se invierte para algunos $x < 10^{10^{10^{34}}}$. En 1955 Skewes, sin usar la RH, mostró la desigualdad $\pi(x) < Li(x)$ invierte para alguno $x < 10^{10^{10^{963}}}$. Tal vez este fue el primer ejemplo en el que un resultado se probó primero asumiendo la RH y más tarde fue demostrado sin asumirla.

3. *Las distancias entre los números primos consecutivos.* En 1919, Cramer mostró que la RH implica que existe una constante $C$ tal que $p_{k+1} - p_k = C\sqrt{p_k}\log p_k$,

donde $p_k$ es el $k$-ésimo primo. Una conjetura de Legendre sostiene que siempre hay un primo entre $n^2$ y $(n+1)^2$, de hecho, deberían existir varios y esto implicaría $p_{k+1} - p_k = C\sqrt{p_k}$. Esto es mejor que el resultado de Cramer, va más allá que una consecuencia de la RH. Cramer también conjeturó que la brecha es realmente $C\,(\log p_k)^2$.

A continuación, presentamos aplicaciones que involucran a la función zeta y $L$-funciones, y no sólo la función zeta de Riemann. Se debe tener en cuenta que tendremos que asumir la GRH para un número infinito de tales funciones para poder decir algo.

1. *La conjetura de Chebyshev.* En 1853, Chebyshev tabuló los números primos que son congruentes a $3 \bmod 4$ y los números primos congruentes a $1 \bmod 4$. Notó que siempre hay al menos tantos primos congruentes a $3 \bmod 4$ hasta un $x$ dado, como primos congruentes a $1 \bmod 4$ y menores o igual a $x$. A partir de la evidencia experimental, conjeturó que esto es siempre verdad y también dió un sentido analítico a la afirmación: hay más primos congruentes a $3 \bmod 4$ que primos congruentes a $1 \bmod 4$. Su conjetura es implicada por la verdad de la igualdad
$$\lim_{x \to 1^-} \sum_{p \neq 2} (-1)^{(p+1)/2} x^p = \infty.$$
Aquí la suma es sobre los números primos impares $p$. En 1917, Hardy-Littlewood y Landau (independientemente) mostraron que esta segunda conjetura de Chebyshev de es equivalente a la GRH para la L-función del carácter no trivial mod 4. En 1994, Rubinstein y Sarnak utilizan simplicidad y la hipótesis de independencia lineal sobre ceros de $L$-funciones para probar algunos resultados acerca de la conjetura de Chebyshev.

2. *La conjetura de Goldbach (1742).* La versión "par", dice que todo entero par $n \geq 4$ es suma de 2 números primos, mientras que la versión "impar", dice que cada entero impar $n \geq 7$ es suma de 3 números primos. Para la mayoría de los matemáticos, la conjetura de Goldbach es la versión par, y, obviamente, esta implica la versión impar ($n - 3$ es par). Se han hecho avances en la versión impar asumiendo GRH. En 1923, bajo la suposición de que todas $L$-funciones de Dirichlet son distintas de cero en el semiplano Re $(s) \geq 3/4 - \varepsilon$, donde $\varepsilon$ esta fijo y es independiente de la $L$-función, Hardy y Littlewood mostraron que la conjetura de Goldbach " impar " es cierta para todo $n$ impar suficientemente grande. En 1937, Vinogradov demostró el mismo resultado sin condiciones,

por lo que fue capaz de eliminar GRH como hipótesis. En 1997, Deshouillers, Effinger, Riele, y Zinoviev demostraron que la conjetura de Goldbach impar es cierta para todos los impares $n \geq 7$ asumiendo GRH. Es decir, la conjetura de Goldbach impar esta completamente demostrada si GRH es cierto. En 2013, Harald Helfgott probó la Conjetura de Goldbach impar sin suponer la GRH.

3. *Pruebas de primalidad en tiempo polinomial.* Por resultados de Ankeny (1952) y Montgomery (1971), si GRH es cierto para toda L-función de Dirichlet entonces el menor número en el complemento de un subgrupo propio $H$ de el grupo de unidades $(\mathbb{Z}/m\mathbb{Z})^\times$ es menor o igual a $C\,(\log m)^2$, donde la constante $C$ es independiente de $m$. En 1985, Bach mostró que, asumiendo la GRH, que esta constante debe ser 2. Es decir, cada subgrupo propio de $(\mathbb{Z}/m\mathbb{Z})^\times$ no contiene algún número entero entre el 1 y $2(\log m)^2$. Dicho de otra manera, si el subgrupo $H$ contiene todos los enteros positivos menores a $2(\log m)^2$, entonces el subgrupo es igual al grupo $(\mathbb{Z}/m\mathbb{Z})^\times$. Si suponemos que todas las L-funciones de Dirichlet no tienen ceros no triviales en el semimplano Re $(s) > 1 - \varepsilon$ entonces el menor elemento de $\mathbb{Z}_m)^\star$que no pertenece a ningún subgrupo propio es menor o igual a $C\,(\log m)^{1/\varepsilon}$. Tomando $\epsilon = 1/2$ se obtiene el resultado anterior, que también se deduce admitiendo GRH.

   En 1976, Gary Miller utilizó esos resultados para mostrar suponiendo la GRH que todas las L-funciones de Dirichlet tiene un test de primalidad en tiempo polinomial. (Implica decidir si un subgrupo de unidades es propio o no.) Poco después, Solovay y Strassen dieron una prueba diferente, utilizando los símbolos de Jacobi, que sólo involucran subgrupos que contienen $-1$, por lo que su prueba "sólo" necesita suponer la GRH para L-funciones de Dirichlet de caracteres pares para tener una prueba de primalidad en tiempo polinomial. (Solovay y Strassen describen su test sólo como una prueba probabilística.)

   En 2002 Agrawal, Kayal y Saxena obtuvieron una prueba de primalidad en tiempo polinomial sin suponer la *GRH*. Este es un buen ejemplo de como la GRH guía a los matemáticos en la dirección de lo que debe ser cierto y luego esperan encontrar una prueba de esos resultados mediante otros métodos.

4. *Anillos euclídeos de enteros.* En 1973, Weinberger demostró que si GRH se supone cierto para las funciones zeta de Dedekind entonces cualquier cuerpo de números con un grupo de unidades infinito (así ignorando el cuerpo de los racionales y el de los imaginarios cuadráticos) es euclidiano si tiene número de

clase 1. Como caso especial, en términos concretos, se obtiene: si $d$ es un entero positivo que no es un cuadrado perfecto, entonces el anillo $\mathbb{Z}[\sqrt{d}]$ es un dominio de factorización única sólo si es Euclidiano. Ram Murty y otros, han avanzado en la dirección de obtener pruebas incondicionales de que la condicion número de clase 1 implica euclidiano. Un caso especialmente llamativo es $\mathbb{Z}[\sqrt{14}]$. Tiene número de clase 1 (Gauss debe haber conocido esto en el siglo 19, en el lenguaje de las formas cuadráticas), entonces debería ser euclidiano. Pero recién en 2004, M. Harper demostró que este anillo cuadrático real particular es euclidiano. De manera que se sabía que $\mathbb{Z}[\sqrt{14}]$ es un anillo con factorizacion única 100 años antes de que se demostrara que es euclidiano!!.

5. *Conjetura de Artin de la raíz primitiva* . En 1927, Artin conjeturó que dado un número entero $a$ que no es $\pm 1$ o un cuadrado perfecto, entonces $a$ es un generador de $(\mathbb{Z}/p\mathbb{Z})^{\times}$ para una cantidad infinita de primos $p$, de hecho, una proporción positiva de tales $p$. Como caso especial, tomando a = 10, esto dice que para un número primo $p$, la fracción $\frac{1}{p}$ tiene período decimal $p-1$ para una proporción positiva de $p$. (Para cualquier primo $p$, el período decimal de $1/p$ es un factor de $p-1$, por lo que este caso especial está diciendo que la mayor selección posible se realiza infinitamente a menudo en un sentido preciso. Una versión más débil de este caso especial se debe a Gauss.) En 1967, Hooley publicó una demostración condicional para la conjetura, asumiendo ciertos casos de la hipótesis generalizada de Riemann. En 1984, R. Gupta y M. Ram Murty mostraron incondicionalmente que la conjetura de Artin es cierta para infinitos $a$ usando métodos de cribado. Roger Heath-Brown mejoró sus resultados y mostró incondicionalmente que existen, como mucho, dos números primos excepcionales para los cuales la conjetura de Artin no es verdad. Este resultado no es constructivo, en lo que se refiere a las excepciones. Por ejemplo, se sigue del teorema de Heath-Brown que uno de los primos 3, 5 ó 7 es una raíz primitiva módulo p para infinitos p. Pero la demostración no proporciona una forma de calcular cual de ellos son.

6. *El primer primo en una progresión aritmética.* Si mcd $(a, m) = 1$ entonces hay infinitos primos $p \equiv a \bmod m$. ¿Cuándo aparece el primero, en función de $m$? En 1934, asumiendo GRH, Chowla mostró que el primer primo $p \equiv a \bmod m$ es menor o igual a $O(m^2(\log m)^2)$. En 1944, Linnik mostró, sin usar GRH que la cota es $O(m^L)$ para algún exponente universal $L$.

7. *Problema número de clase de Gauss.* Gauss (1801) conjeturó, en el lenguaje de formas cuadráticas, que sólo hay un número finito de cuerpos cuadráticos a imaginarios con número de clase 1. (En realidad conjeturó más precisamente que los nueve ejemplos conocidos son los únicos) En 1913, Gronwall mostró que esto es cierto si las $L$-funciones de todos los caracteres de Dirichlet cuadráticos imaginarios no tienen ceros en alguna franja común $1 - \varepsilon < \mathrm{Re}\ (s) < 1$. Esto es más débil que GRH (sólo se preocupan por L-funciones de una colección de caracteres restingidos), pero aún así es una condición sin demostración. En 1933, Deuring y Mordell demostraron que la conjetura de Gauss es cierto si la RH (para la función zeta de Riemann) es falsa, y luego en 1934 Heilbronn demostró que la conjetura de Gauss es cierta si la GRH es falsa para alguna L-funcióne de Dirichlet de un carácter cuadrático imaginario. Como Gronwall probó la conjetura de Gauss si GRH es cierta para la función zeta de Riemann y L-funciones de Dirichlet de todos los caracteres cuadráticos imaginarios de Dirichlet, y Deuring - Mordell - Heilbronn demostraron que la conjetura de Gauss es cierta si GRH es falsa para al menos una de estas funciones, luego la connjetura de Gauss es cierta por lógica elemental. En 1935, Siegel probó la conjetura de Gauss sin condiciones, y en los años 1950's y 1960's Baker, Heegner, y Stark dieron pruebas independientes y separadas de la conjetura de Gauss más precisa, en la que se establece que los nueve ejemplos conocidos son los únicos.

8. *Los valores perdidos de una forma cuadrática.* Lagrange (1772) mostró que todo entero positivo es la suma de cuatro cuadrados. Sin embargo, no todo entero es una suma de tres cuadrados $x^2+y^2+z^2$ es un entero que no satisface $n \equiv 7 \bmod 8$. Legendre (1798) mostró que un número entero positivo es la suma de tres cuadrados si y sólo si no es de la forma $4^a(8k + 7)$. Esto se puede expresar como un problema local-global, esto es, $x^2 + y^2 + z^2 = n$ tiene solución en los números enteros si y sólo si la congruencia $x^2 + y^2 + z^2 \equiv n \bmod m$ tiene solución para todo $m$. Más en general, el mismo fenómeno local-global vale para la forma cuadrática de tres variables $x^2 + y^2 + c\,z^2$ para todos los enteros $c$ de 2 a 10, excepto $c = 7$ y $c = 10$. ¿Qué sucede para estos dos valores especiales? Ramanujan estudió el caso $c = 10$. Encontró 16 valores de $n$ para los que hay solución local (es decir, que podemos resolver $x^2 + y^2 + 10\,z^2 \equiv n \bmod m$ for todo $m$) pero no hay solución global (no hay solución entera para $x^2 + y^2 + 10\,z^2 = n$). Dos valores adicionales de $n$

se encontraron más tarde, y en 1990 Duke y Schulze-Pillot mostraron que la existencia de solución local implica existencia de solución global a excepción de un número finito de números enteros positivos $n$. En 1997, Ono y Soundarajan mostraron que, asumiendo la GRH, las 18 excepciones conocidas son las únicas.

9. *Los números convenientes de Euler.* Euler llama un número entero $n \geq 1$ conveniente si cualquier número entero impar mayor que 1 que se puede representar de manera única como $x^2 + n\,y^2$ para enteros positivos $x$ e $y$, que satisfacen $(x, ny) = 1$. Estos números fueron utilizados por Euler para probar que ciertos números que eran grandes en su época, como por ejemplo $67.579 = 229^2 + 2 \cdot 87^2$, son primos. Euler encontró 65 números convenientes menores a 10.000 (el último es 1848). En 1934, Chowla mostró que hay un número finito de números convenientes. En 1973, Weinberger mostró que hay a lo sumo un número conveniente que no está en la lista de Euler, y si las $L$-funciones de todos los caracteres de Dirichlet cuadráticos satisfacen GRH entonces la lista de Euler es completa. Lo que se usa de la GRH es la falta de ceros reales en el intervalo $(\frac{53}{54}, 1)$.