¿DÓNDE ESTÁN LOS NÚMEROS PRIMOS?

WHERE ARE THE PRIME NUMBERS?

Federico Menéndez Conde Lara.[1]

Resumen

Se presenta una vista panorámica de los resultados históricos que se han obtenido en el estudio sobre cómo están distribuidos los números primos. Se incluyen algunos resultados muy recientes.

Palabras clave: teoría de números, números primos, distribución asintótica, función zeta de Riemann, panorama histórico

Abstract

We present a general overview of the historical results concerning the distribution of prime numbers. Some recent developments are mentioned.

Keywords: number theory, prime numbers, asymptotic distribution, Riemann zeta function, historic overview

INTRODUCCIÓN

Los números primos han despertado la curiosidad humana desde tiempos muy remotos. En particular, la cuestión de describir cómo están distribuidos dentro de los números enteros ha sido abordada a través de los siglos por una cantidad considerable de los matemáticos más célebres de la historia.

¿Qué es lo que hace tan relevante dicha cuestión? Un primer vistazo al inicio de esta secuencia, que es infinita, parece sugerirnos una pista:

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,\ldots$$

¿Hay un patrón en esa secuencia? La mente humana está acostumbrada a encontrar patrones y reglas, incluso donde no los hay, pero la secuencia de los números primos se resiste a cualquier intento de identificar alguno. Los primos van apareciendo de forma caprichosa, sin ningún orden aparente.

Existen algunas restricciones para la secuencia, emanadas de la propia definición de número primo: por ejemplo, no puede haber dos números consecutivos que sean primos (excepto por 2 y 3), ni tampoco puede haber tres impares consecutivos que lo sean (excepto por 3, 5 y 7). Salvo por ese tipo de limitantes, los números primos parecen irse sucediendo unos a otros de manera aleatoria. Y sin embargo, su

definición es por completo determinista. Desde la antigüedad hasta nuestros días, las preguntas relacionadas con buscar dónde están los números primos ha sido objeto de una intensa búsqueda de respuestas, y fuente de una abundante cantidad de trabajos de investigación. Cabe mencionar que, si bien el interés por los números primos es ancestral, es a partir de los siglos XVIII y XIX que el interés por estudiar la distribución de los números primos tiene un avance mucho más considerable, situación que va de la mano del notable desarrollo de las matemáticas que tuvo lugar en ese tiempo. Muchas cosas acerca de ellos se han logrado demostrar acerca de la forma en que los números primos están distribuidos. En no pocos casos esto se ha conseguido con el uso de herramientas inesperadas, que revelan la existencia de profundas conexiones de la aritmética con otras ramas de las matemáticas. Por otra parte, no pocos de los comportamientos observados resultan ser en apariencia contradictorios entre sí. Todo ello ha aumentado el aura de misterio que rodea a los números primos, acentuando el interés por buscarlos.

En este breve artículo se pretende presentar algunos de los resultados más importantes que se han obtenido en esta dirección. Algunos de estos resultados son ya antiguos, mientras que otros son muy recientes. Como podremos ver, es mucho y muy profundo lo que se conoce; pero es claro también que es mucho más lo que queda todavía por conocer.

PRELIMINARES

En esta sección presentamos la definición de número primo y unas pocas de sus propiedades básicas que serán referidas en secciones posteriores. Todos los resultados que presentamos a en esta sección eran conocidos desde la antigua Grecia, y están incluidos – con sus demostraciones respectivas – en los Elementos de Euclides.

Usaremos la notación usual $\mathbb{N}$ para el conjunto de los enteros positivos $\{1,2,3,4,\dots\}$, también llamados *números naturales*. Dados dos números naturales a y b, se dice que a es *divisor* de b si existe un natural k tal que $b = ak$. En otras palabras, a es divisor de b cuando la fracción b/a es igual a un número entero. Es claro que el número 1 es divisor de todos los enteros, y que todo entero es divisor de sí mismo. También, para que a sea divisor de b resulta necesario que $a \leq b$. Se dice que un número natural $p > 1$ es un *número primo* si no tiene otros divisores aparte de 1 y p. Es decir, p es primo si al dividirlo entre cualquier otro número natural, distinto de 1 y p, el resultado no es entero. Por ejemplo, el número 5 es primo ya que ninguno de los números $5/2$, $5/3$ y $5/4$ es entero. Pero 12 no es primo porque $12/3 = 4$ sí es un número entero; notemos que eso es equivalente a que el número 12 sea igual al producto de los enteros 3 y 4. Es decir, un número no es primo si y solo si puede expresarse como el producto de dos enteros positivos menores a él. A los números que no son primos se les conoce con el nombre de *números compuestos*.

A continuación presentamos tres resultados fundamentales acerca de los números primos. El primero de ellos se conoce como el *lema de Euclides*, y corresponde a las proposición 30 del Libro VII de los Elementos (Euclides, 2005).

Teorema 1. *Si un primo p es divisor del producto de dos números enteros, entonces p es divisor de al menos uno de ellos dos.*

Para demostrar el lema de Euclides, supongamos que p es divisor del producto ab y que no es divisor de a; queremos mostrar que p es divisor de b. Por definición de divisor, existe un entero k tal que $pk = ab$, lo que nos lleva a la igualdad de fracciones

$$\frac{p}{a} = \frac{b}{k}.$$

Ahora bien: la fracción de la izquierda no puede reducirse, puesto que p y a no tienen ningún divisor común mayor a 1. Entonces la fracción del lado derecho de la igualdad debe poder reducirse para que sea igual a la del lado izquierdo; esto implica que existe un entero n tal que $b = np$, y tenemos que p divide a b, como se quería.

Una consecuencia casi inmediata del lema de Euclides, correspondiente a las proposiciones 31 y 32 del Libro VII, es:

Teorema 2. *Todo número entero tiene un divisor que es primo.*

En efecto, supongamos que hubiera números naturales sin divisores primos. Entonces, de entre todos esos tendría que haber uno que es el menor: llamémosle m. Este número m tiene que ser compuesto, pues si fuera primo ya tendría un divisor primo (él mismo). Digamos entonces que $m = ab$, con $1 < a \leq b < m$. Por definición de m, dado que $a < m$, se tiene que a tiene un divisor primo (y lo mismo para b). Digamos que $a = pc$ con p un primo y c entero. Se sigue que $m = p(cb)$ de modo que p es también divisor de m, lo que contradice el hecho de que m no tenga divisores primos.

El siguiente teorema, conocido con el llamativo nombre de *teorema fundamental de la aritmética*, nos dice que los números primos son una especie de bloques, a partir de los cuales podemos construir a todos los números enteros. Además nos dice que cada número tiene su muy particular elección de bloques que no puede ser sustituida por ninguna otra. Este teorema corresponde a la proposición 14 del Libro IX de los Elementos.

Teorema 3. *Todo número entero $n \geq 2$ puede descomponerse como un producto de la forma*

$$n = p_1 \cdot p_2 \cdots p_r$$

donde $p_1, p_2, \ldots, p_r$ son números primos (no necesariamente distintos). Además, la elección de los p_j es única salvo por reordenamiento de los mismos.

Por ejemplo, la descomposición del número 2016 está dada por $2016 = 2^5 \cdot 3^2 \cdot 7$, mientras que el número 2017 es primo. Para demostrar el teorema fundamental de la aritmética hay que probar dos cosas: que la descomposición existe y que es única. La existencia puede demostrarse mediante el método de *descenso infinito*: sea n un entero positivo cualquiera. Si n no es primo, el teorema 2 nos garantiza que $n = p_1 \cdot n_1$, para algún primo p_1 y algún $n_1 < n$. De la misma manera, si n_1 no es primo existen un primo p_2 y un entero $n_2 < n_1$ tal que $n = p_1 \cdot n_1 = p_1 \cdot p_2 \cdot n_2$. Y así, podemos continuar este proceso obteniendo una secuencia de enteros $n > n_1 > n_2 > \cdots > n_k$ y primos $p_1, \ldots, p_k$ para los cuales se tiene que $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k \cdot n_k$. Ahora bien, este proceso debe terminar en algún momento ya que en caso contrario se tendría una sucesión decreciente infinita de números naturales n_j lo que claramente no es posible; es decir, algún n_j deberá ser primo y concluimos el resultado buscado.

A continuación probamos la unicidad. Supongamos para ello que

$$n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$$

donde los p_j y los q_j son números primos. Queremos verificar que $r = s$ y que los q_j y los p_j son los mismos números (tal vez distinto orden). Un repetido uso del lema de Euclides nos da el resultado: como p_1 es divisor del producto $q_1 \cdot q_2 \cdots q_s$, necesariamente tiene que ser divisor de algún q_j, y como p_1 y q_j son primos se tiene que deben ser iguales. Pongamos que este q_j es igual a q_1 (renombrando los q's si fuera necesario). Continuamos este procedimiento, ahora con p_2: como divide a $q_2 \cdots q_s$ tiene

que ser igual a alguno de esos factores que, digamos q_2 (sin pérdida de generalidad). Y así, repitiendo dicho procedimiento hasta p_r se tiene que $p_j = q_j$ para cada $j = 1, \ldots, r$. En particular, $r \leq s$. Pero como podemos proceder también en sentido inverso (intercambiando el papel de las p_j y las q_j) se sigue que $s \leq r$, y por lo tanto $s = r$ y ambas descomposiciones son iguales.

CONTANDO A LOS NÚMEROS PRIMOS

En la búsqueda de la forma en que los números primos están distribuidos dentro de los números enteros, una pregunta que resulta natural es:

¿Cuántos números primos hay?

Una respuesta inmediata a esta pregunta es que el conjunto de los números primos es infinito. Este hecho, conocido desde la antigüedad, puede demostrarse con un argumento breve y elemental:

Supongamos que $X = \{p_1, p_2, \ldots, p_N\}$ es un conjunto finito de números primos, y consideramos el producto de todos ellos:

$$P = p_1 \cdot p_2 \cdot p_3 \cdots p_{N-1} \cdot p_N.$$

El número $P+1$ es desde luego distinto que todos los primos del conjunto al ser mayor que todos ellos. Pero al dividir $P+1$ entre cualquiera de ellos el residuo es igual a 1, de forma que ninguno de los primos en X divide a $P+1$. Por otra parte por el teorema 2 existe un primo que sí divide a $P+1$. Luego entonces, tenemos que hay un número primo que no está en el conjunto X y hemos de concluir que ningún conjunto finito puede contener a todos los números primos. El conjunto de los números primos tiene que ser por lo tanto infinito.

Una demostración de la existencia de infinitos números primos aparece en la proposición 20 del Libro IX de los Elementos de Euclides. Dicha prueba es en esencia la misma que presentamos arriba, aunque Euclides no hace referencia explícita al infinito, sino que afirma simplemente que ninguna colección de números primos *de cualquier magnitud* puede contenerlos a todos (Euclides, 2005). En cierto sentido el resultado anterior responde del todo a la pregunta que se plantea al principio de la presente sección. En particular, eso es lo que ocurre de acuerdo a la *teoría de conjuntos*, introducida por Georg Cantor a fines del siglo XIX. Entre otras cosas, esta teoría se ocupa de clasificar a los conjuntos con un número infinito de elementos de acuerdo a su tamaño (la palabra usada para referirse al número de elementos de un conjunto es su *cardinalidad*); en otras palabras, en la teoría de conjuntos se considera que existen distintos infinitos, y que algunos de ellos son más grandes que otros. De entre todas esas cardinalidades infinitas, la menor de todas corresponde a la del conjunto de los números enteros y se denota por $\aleph_0$ (que se lee "alef cero"). Una consecuencia de esto es que todo subconjunto infinito de los enteros tendrá la misma cardinalidad $\aleph_0$. Desde ese punto de vista hay la misma cantidad de números pares que de cuadrados perfectos, y la misma cantidad de cuadrados perfectos que de múltiplos de 20, y la misma cantidad de múltiplos de 20 que de números primos: todos ellos son subconjuntos infinitos de los enteros. Sin embargo, resulta claro que estas consideraciones son insuficientes si lo que queremos es describir apropiadamente a estos conjuntos, y la forma en que están distribuidos dentro de los naturales. No parece muy aventurado el afirmar, por ejemplo, que hay más números pares que múltiplos de 20, y que hay más múltiplos de 20 que cuadrados perfectos. Eso es lo que parece dictar el sentido común. Sin embargo, en matemáticas el sentido común no es suficiente y al final del día se requiere establecer las cosas de manera precisa. La cuestión que se nos presenta es entonces: proponer una forma de medir subconjuntos

infinitos de enteros que detecte estas diferencias, resultando más adecuada para la pregunta que nos hemos planteado al inicio de esta sección. A continuación le daremos un sentido preciso a esta consideración.

Apelando a la intuición, no es difícil que estemos de acuerdo en que "la mitad de los números enteros es par" y que "la vigésima parte de los números enteros es múltiplo de 20." Es en este sentido que entendemos que hay más pares que múltiplos de 20, y si bien es cierto que en un principio pareciera no tener sentido el hablar de "la mitad de infinito" o "la vigésima parte de infinito", todo esto puede hacerse matemáticamente riguroso mediante un sencillo artificio.

Definicion 1. *Sea X un subconjunto de $\mathbb{N}$, y para $n \in \mathbb{N}$ sea $N_X(n)$ la cantidad de elementos de X que son menores o iguales que n. Si existe el límite*

$$d(X) = \lim_{n\to\infty} \frac{N_X(n)}{n}$$

llamamos a $d(X)$ la densidad asintótica de X.

Esto es: en vez de hablar directamente de fracciones de infinito (lo que en sí mismo no tendría sentido), le sacamos la vuelta al asunto contando el número de elementos del conjunto que están en el conjunto finito $\{1,2,3,\ldots,n-1,n\}$ y observando cuál es la proporción. Observamos lo que sucede al hacer n más y más grande, es decir "hacer n tender a infinito". Si la proporción converge a alguna cantidad, a esa cantidad le llamamos la *densidad asintótica* del conjunto. Habiendo establecido lo anterior, no es difícil convencernos de que el conjunto de los múltiplos de un número fijo m tiene densidad asintótica igual a $1/m$. Más en general, la densidad asintótica N_X es un número entre 0 y 1 que describe la proporción de elementos de X dentro de los naturales. Mientras más grande sea su valor, más grande es el conjunto; en particular, el conjunto mismo de los naturales tiene densidad asintótica igual a 1, mientras que el conjunto de los cuadrados perfectos tiene densidad asintótica igual a 0. En vista de esto y regresando a nuestro objeto de interés que son los números primos, la pregunta sobre *cuántos números primos hay* vuelve a cobrar sentido e interés: ya sabemos que son infinitos, pero *¿cuál es su densidad asintótica?*

Existen en realidad muchas formas distintas y razonables de determinar el tamaño de un subconjunto infinito de $\mathbb{N}$ (Barlow and Taylor, 1989). La presentada en el párrafo anterior se distingue por su naturalidad y sencillez, pero tiene un inconveniente importante: no distingue apropiadamente entre algunos conjuntos. En particular, esto es lo que ocurre con conjuntos de densidades asintóticas iguales a 0 (es decir, para conjuntos infinitos pequeños). Para concretizar lo que se quiere decir: notemos que – como ya señalamos antes – el conjunto de los cuadrados perfectos tiene densidad asintótica 0. Lo mismo ocurre para los cubos perfectos, y para las potencias de cualquier número n. Y retornamos a un dilema similar al que teníamos con la cardinalidad: la intuición nos dice que debería haber más cuadrados que cubos, y más cubos que potencias de cien... pero todos esos conjuntos tienen la misma densidad asintótica (igual a cero). Afortunadamente, el nuevo dilema con el que nos encontramos tiene una salida que consiste en refinar la idea de densidad asintótica. Presentamos esto en la siguiente definición.

Definicion 2. *Sean $a(n)$ y $b(n)$ dos funciones definidas en $\mathbb{N}$. Diremos que son asintóticamente equivalentes, y lo denotamos por $a \sim b$, si*

$$\lim_{n\to\infty} \frac{a(n)}{b(n)} = 1$$

En el caso en que X y Y sean dos subconjuntos de $\mathbb{N}$ tales que las funciones $N_X(n)$ y $N_Y(n)$ sean asintóticamente equivalentes, también diremos que X y Y lo son. Denotamos esto también por $X \sim Y$.

Una observación sencilla es que si las dimensiones asintóticas de X y de Y son iguales y positivas, entonces los conjuntos son asintóticamente equivalentes. En efecto, si $d(X) = d(Y) = c > 0$, entonces

$$\begin{aligned}\lim_{n\to\infty} \frac{N_X(n)}{N_Y(n)} &= \lim_{n\to\infty} \frac{N_X(n)/n}{N_Y(n)/n} \\ &= (1/c)/(1/c) \\ &= 1.\end{aligned}$$

En cambio, no ocurre lo mismo en el caso cuando ambas densidades asintóticas son iguales a cero. Por ejemplo, si X es el conjunto de cubos perfectos y Y es el conjunto de los cuadrados perfectos, es fácil ver que

$$\lim_{n\to\infty} \frac{N_X(n)}{N_Y(n)} = 0. \tag{1}$$

La igualdad (1) nos dice que, así interpretado, el conjunto X de los cubos perfectos es más pequeño (mucho más pequeño, de hecho) que el conjunto Y de los cuadrados perfectos. Una termonología usual para decir la misma cosa (conocida como *notación de Landau*), es decir que $N_X(n)$ es una *o pequeña* de $N_Y(n)$. Esto se denota por $N_X(n) = o(N_X(n))$.

El siguiente resultado, que es un teorema en extremo célebre y del que trataremos con algo más de detalle en la próxima sección, nos da respuesta a la pregunta que planteamos acerca de la cantidad de números primos, entendiendo esta en los términos de equivalencia asintótica que se han propuesto. Denotaremos al conjunto de los números primos por $\mathscr{P}$. Usaremos la expreión $\pi(x)$, usual en la literatura, para denotar al número de primos menores o iguales que x. En otras palabras $\pi(n) \equiv N_{\mathscr{P}}(n)$.

Teorema 4. (Teorema de los números primos).

$$\pi(n) \sim \frac{n}{\log(n)}.$$

El logaritmo en este teorema corresponde al llamado *logaritmo natural* (al logaritmo en base e). Lo que nos dice el teorema de los números primos es que dentro del conjunto de los números $\{1, 2, \ldots, n\}$ la proporción de ellos que son primos es aproximadamente igual a $1/\log(n)$, siempre y cuando el número n sea grande. Como $\log(n)$ crece indefinidamente (se va a infinito), se tiene que la proporción de números primos se va haciendo cada vez más y más pequeña; menor que cualquier $1/m$ dado si nos alejamos lo suficiente. En consecuencia se tiene que la densidad asintótica de los números primos es igual a 0. Visto de este modo, podría decirse que hay muy pocos números primos: menos que los múltiplos de un número fijo m, por grande que este sea. De manera más elocuente, aunque bastante informal, en cierta forma podemos decir que "menos de una millonésima parte de los naturales son primos". O menos de una billonésima parte, o menos de una trillonésima parte, etc.

Como ya mencionamos antes, la anterior no es la única forma de medir el tamaño de un subconjunto de $\mathbb{N}$. Otra forma que puede proponerse, en principio una muy razonable, es considerar la suma de sus recíprocos multiplicativos. Esto es, si $\{a_1, a_2, a_3, \ldots\}$ son los elementos de un conjunto A, entonces la suma

$$\sum_{n=1}^{\infty} \frac{1}{a_n} = \frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \cdots \tag{2}$$

es un indicador del tamaño del conjunto A: mientras más dispersos estén los números del conjunto, los términos de la suma serán más pequeños. Para ilustrar esto, consideremos el conjunto de las potencias

del número 2. En ese caso la suma (2) es

$$\sum_{n=1}^{\infty} \frac{1}{2^n} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots = 1.$$

Más en general, si consideramos el conjunto de las potencias de un entero $a > 1$ fijo obtenemos la llamada *serie geométrica*

$$\sum_{n=1}^{\infty} \frac{1}{a^n} = \frac{1}{a} + \frac{1}{a^2} + \frac{1}{a^3} + \frac{1}{a^4} + \cdots = \frac{1}{a-1}. \tag{3}$$

Para mostrar la validez de esta igualdad, consideramos las sumas parciales finitas

$$S_N = \frac{1}{a} + \frac{1}{a^2} + \frac{1}{a^3} + \frac{1}{a^4} + \cdots + \frac{1}{a^N}.$$

Se tiene que

$$S_N - \frac{1}{a} \cdot S_N = \left(\frac{1}{a} + \frac{1}{a^2} + \frac{1}{a^3} + \cdots + \frac{1}{a^N} \right) - \left(\frac{1}{a^2} + \frac{1}{a^3} + \cdots + \frac{1}{a^{N+1}} \right)$$

$$= \frac{1}{a} - \frac{1}{a^{N+1}}.$$

Despejando S_N, haciendo $N \to \infty$ y simplificando la expresión, se obtiene la igualdad (3). Como es de esperarse, conforme el número a sea más grande, su suma correspondiente $1/(a-1)$ va a ser menor, lo que está de acuerdo con el hecho de que el conjunto de las potencias de a es más pequeño (o mejor dicho, está más disperso) cuando el valor de a es más grande.

En el extremo opuesto a la serie geométrica está la llamada *serie armónica*, que corresponde a cuando el conjunto A es el más grande subconjunto posible de los naturales. Esto es, cuando $A = \mathbb{N}$. En dado caso se tiene

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

y no es difícil ver que esta suma es más grande que todos los números naturales (es decir, diverge hacia infinito). Una forma rápida de ver esto consiste en escribir la suma agrupando términos de la siguiente manera:

$$1 + \left(\frac{1}{2} + \frac{1}{3} \right) + \left(\frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} \right) + \cdots + \left(\frac{1}{2^n} + \cdots \frac{1}{2^{n+1} - 1} \right) + \cdots$$

Cada una de las sumas que quedan entre paréntesis es mayor a $1/2$, y como hay infinitos de estos términos la suma total debe ser infinita. En efecto, si M es cualquier entero positivo, tomar los primeros $2M+1$ términos basta para garantizar que la suma de ellos es mayor que M.

Una situación intermedia entre la series geométrica y la serie armónica es la que ocurre cuando el conjunto A está formado por los cuadrados perfectos o por cubos perfectos o en general por las potencias de algún orden $m \geq 2$ fijo. En ese caso, la suma es

$$\sum_{n=1}^{\infty} \frac{1}{n^m} = 1 + \frac{1}{2^m} + \frac{1}{3^m} + \frac{1}{4^m} + \cdots \tag{4}$$

que es fácil comprobar que dicha suma converge a algún número finito. Puede ser muy sorprendente el hecho de que el determinar el valor de ese número sea un problema en extremo complicado. En el caso $m = 2$ se tiene el famoso *problema de Basilea* cuya solución fue encontrada por Leonhard Euler en el siglo XVIII y que establece que

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6}.$$

El problema de Basilea es de una gran notoriedad e interés histórico; hay muchas fuentes en las que podemos encontrar información más detallada sobre esto; por ejemplo, podemos referir a (Grabinsky, 2007), (Sánchez Muñoz, 2014) y (Barrera Fragoso and Rojas Chavarría, 2017). Para los otros valores pares de m, se conocen expresiones cerradas para las sumas en términos de potencias del número π y de los llamados *números de Bernoulli*. En el caso $m = 3$ al valor de la suma se le conoce como *constante de Apéry*, en honor del matemático que demostró que dicho número es irracional (Apéry, 1979). No se sabe si la constante de Apéry es trascendente. Si $m = 5$ no se sabe siquiera si el valor es irracional o no (aunque se sabe que para infinitos valores impares de m el valor de la suma es irracional). Para una extensa discusión sobre este tema referimos a (Waldschmidt, 2009).

Regresando a la cuestión central que nos ocupa, nos preguntamos qué es lo que pasa con la serie (2) en el caso en el que A es el conjunto de los números primos. Esta pregunta fue respondida también por Euler (1737), y tal vez resulte sorprendente el hecho de que

$$\sum_{p \in \mathscr{P}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots = +\infty. \tag{5}$$

Es decir, de acuerdo a esta forma de medir, el conjunto de los números primos resulta ser muy grande. Esto se contrapone con el hecho observado arriba de que la densidad asintótica de los primos es igual a cero. Este tipo de contradicciones aparentes son muy frecuentes en el estudio del comportamiento de los números primos.

La demostración ideada por Euler para la divergencia de la serie (5) está basada en una observación que relaciona a las sumas (4) con un producto infinito que involucra a los recíprocos de los números primos. Esta relación, conocida como la *fórmula del producto de Euler* está dada por

$$\sum_{n=1}^{\infty} \frac{1}{n^m} = \Pi \left(\frac{1}{1 - \frac{1}{p^m}} \right) \tag{6}$$

donde el producto de la derecha se toma sobre todos los números primos p. Para obtener la igualdad (6) notemos primero que aplicando la serie geométrica (3) para $a = p$, obtenemos

$$\begin{aligned} \frac{1}{1 - \frac{1}{p^m}} &= \frac{p^m}{p^m - 1} \\ &= 1 + \frac{1}{p^m - 1} \\ &= 1 + \frac{1}{p^m} + \frac{1}{p^{2m}} + \frac{1}{p^{3m}} + \frac{1}{p^{4m}} + \cdots \end{aligned}$$

Así, si multiplicáramos todos estos factores – sobre todos los primos – obtendríamos precisamente la suma de los términos $1/n$, ya que cada natural aparece exactamente una vez: la correspondiente a

su descomposición en primos que nos da el teorema fundamental de la aritmética (teorema 3). Una vez establecido lo anterior, tomamos logaritmos de ambos lados de la igualdad (6) con $m = 1$ para obtener que

$$\log\left(\sum_{n=1}^{\infty}\frac{1}{n}\right) = -\sum_{p\in\mathscr{P}}\log\left(1-\frac{1}{p}\right).$$

Usando la expansión en serie de Taylor de la función $\log(x)$, y reagrupando términos se obtiene que

$$\sum_{p\in\mathscr{P}}\frac{1}{p} = \log\left(\sum_{n=1}^{\infty}\frac{1}{n}\right) - \sum_{p\in\mathscr{P}}\frac{1}{p^2} - \sum_{p\in\mathscr{P}}\frac{1}{p^3} - \sum_{p\in\mathscr{P}}\frac{1}{p^4} - \cdots$$

Como sabemos, la primera de las sumas infinitas del lado derecho de la igualdad es divergente, y es claro que todas las demás son convergentes. Por lo tanto la suma de la izquierda debe ser infinita, y se obtiene el resultado enunciado.

Una objeción a la forma de medir subconjuntos usando la serie (2) es que al darle mucho peso a los primeros elementos de $\mathbb{N}$, puede otorgar una medida "demasiado grande" a conjuntos que digamos que "no deberían ser grandes". Para poner un ejemplo: el conjunto de solo dos elementos $\{1,2\}$ mide $3/2$, por lo que resulta ser mayor que el conjunto de pontencias positivas de 2 descrito arriba. Cabe aclarar que este dilema desaparece cuando tratamos con series divergentes. En otras palabras: el que el valor de la serie sea infinito sí nos dice de una manera bastante apropiada que el conjunto A es grande (más grande en un sentido importante que cualquier conjunto que diera un valor finito de la suma).

EL TEOREMA DE LOS NÚMEROS PRIMOS

El teorema 4 fue conjeturado por Adrien–Marie Legendre, a partir de observaciones empíricas, a finales del siglo XVIII. La demostración rigurosa del mismo no llegó sino hasta un siglo más tarde, siendo probado el mismo año, de manera independiente, por Jacques Hadamard (1896) y Charles–Jean De la Vallée Poussin (1896). El progreso que llevó a la demostración de este teorema constituye uno de los capítulos más notables en la historia de las matemáticas, y dicho resultado ha llegado a ser considerado "el resultado más sorprendente en matemáticas" (Apostol, 2001). Cabe mencionar que lo sorprendente de este teorema no es el resultado en sí, sino los métodos usados en la demostración del mismo. Tanto Hadamard como De la Vallée Poussin emplearon métodos de una rama de las matemáticas conocida como *análisis complejo* que, en términos generales, consiste en trasladar las ideas del cálculo (análisis real) a funciones de variable compleja. Es decir, funciones definidas sobre los números complejos, aquellos de la forma $a+ib$, donde i es la unidad imaginaria que satisface $i^2 = -1$, mientras que a y b son números reales. El análisis complejo ha resultado tener profundas implicaciones en diversas áreas no solo dentro de las matemáticas puras, sino que ha resultado muy útil en no pocas aplicaciones, tan diversas como ingeniería eléctrica, mecánica de fluidos, relatividad general, telecomunicaciones y teoría de control, por mencionar algunas. De manera todavía más notable, el análisis complejo ha mostrado tener profundas conexiones con diversas áreas de las matemáticas, muchas veces de formas muy sorprendentes. La teoría de números es tal vez el mejor ejemplo de ello: para resolver un problema particular de aritmética, concerniente en principio solo a los números enteros, los métodos que resultaron más eficientes resultaron del surgimiento de una teoría analítica sobre los números complejos. La teoría clásica del análisis complejo se desarrolló en la segunda mitad del siglo XIX, y el teorema de los números primos fue uno de los motores que guiaron este desarrollo (Grey, 2015). Nos resulta por demás sugestivo el que el afán por resolver un problema

de aritmética tuviera como consecuencia el desarrollo de una teoría con un sinnúmero de implicaciones en las ciencias, tanto puras como aplicadas. Para una discusión mucho más extensa y detallada que lo que podemos presentar aquí de la historia del teorema de los números primos y de su gran impacto, referimos a (Fine and Rosenberger, 2010). Una presentación detallada de las demostraciones completas de Hadamard y de De la Vallée Poussin puede encontrarse en el libro de H.M. Edwards (2001) sobre la función zeta de Riemann.

El teorema de los números primos es en muchos sentidos el punto de partida de lo que hoy se conoce como la *teoría analítica de números* (Apostol, 1998). Un momento crucial en la historia de su demostración fue la aparición del breve artículo de Bernhard Riemann titulado "Sobre el número de primos menores que una cantidad dada" (Riemann, 1859). Este artículo está considerado uno de los más importantes en la historia de las matemáticas. Es en ese artículo en el que Riemann propone su famosa conjetura acerca de la función zeta, conocida como la *hipótesis de Riemann* y que es generalmente propuesto como el problema sin resolver más reconocido en matemáticas; se puede afirmar incluso, que existe un amplio consenso sobre esto. En ese artículo, Riemann consideró la fórmula del producto de Euler (6) de una manera más general: el parámetro m, que para Euler era un número entero positivo, es sustituido por una variable s que toma valores complejos (con parte real mayor a 1). La suma en el lado izquierdo de esa igualdad es conocida ahora como la *función zeta de Riemann*, usualmente denotada por $\zeta(s)$ y definida por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad s \in \mathbb{C}, \quad \mathrm{Re}(s) > 1. \tag{7}$$

Para valores de s con parte real menor o igual a uno, la serie de arriba es divergente. Riemann buscó una expresión para $\zeta(s)$ que fuera válida en todo el plano complejo, llegando a encontrar

$$\zeta(s) = \frac{1}{2\pi i} \left(\int_0^{\infty} e^{-x} x^{-s}\, dx \right) \left(\int_{\gamma} \frac{(-x)^s}{e^x - 1}\, dx \right) \tag{8}$$

donde γ es una curva que comienza en $+\infty$, recorriendo la recta real positiva de forma decreciente, rodea al cero en sentido opuesto a las manecillas del reloj y regresa a $+\infty$ recorriendo la recta real positiva de forma creciente. La expresión (8) resulta ser válida para todos los valores de $s \in \mathbb{C}$ y coincide con la expresión (7) en el dominio Re $(s) > 1$. Además, los valores de $\zeta(s)$ son finitos, salvo por la única excepción cuando $s = 1$. En la terminología del análisis complejo, la función $\zeta(s)$ definida en (8) es una *función meromorfa* que tiene un único *polo simple* en $s = 1$. También de acuerdo a la teoría del análisis complejo (en buena parte desarrollada después y a partir de Riemann), esto se corresponde con el concepto de *extensión analítica* de una función. En términos mundanos lo que esto quiere decir es que de un modo fundamental la expresión (8) es no solo una extensión de (7) sino la única forma de extenderla de manera razonable. Es posible verificar que la función zeta de Riemann $\zeta(s)$ es igual a cero cuando s es un entero negativo par. Referimos al capítulo 1 de (Edwards, 2001) para una derivación formal de este hecho y de la expresión (8). La hipótesis de Riemann consiste en la afirmación (hecha por Riemann un poco de pasada y sin darle mayor importancia) de que todos los demás ceros de la función zeta tienen parte real igual a $1/2$. Esta afirmación ha resultado tener profundas implicaciones, y ser inimaginablemente difícil de demostrar. Ya al iniciar el siglo XX, había sido identificada su considerable importancia y David Hilbert la incluyó en su famosa lista de problemas abiertos (Hilbert, 1902). Un siglo más tarde, fue también incluida en la lista de los siete *problemas del milenio* del Instituto Clay (CMI, 2000). Además de haber sumado evidencia a la conjetura del teorema de los números primos, Riemann señaló el camino a seguir, sentando las bases de las demostraciones que llegaron unas décadas más tarde.

Tanto Hadamard como De la Vallée Poussin expresaron el teorema de los números primos en términos

de la llamada integral logarítmica $\mathrm{Li}(x)$:

$$\pi(x) \sim \mathrm{Li}(x) \equiv \int_2^\infty \frac{dt}{\log(t)}. \tag{9}$$

Dicha relación asintótica había sido conjeturada por Gauss y por Dirichlet, con cerca de un siglo de anterioridad. La relación (9) es equivalente al enunciado del teorema 4 debido a que $\mathrm{Li}(x) \sim x/\log(x)$. Esto se sigue de efectuar una simple integración por partes. De hecho, si integramos por partes repetidas veces obtenemos

$$\mathrm{Li}(x) = \frac{x}{\log(x)} + \frac{x}{\log^2(x)} + \frac{x}{\log^3(x)} + \cdots \tag{10}$$

Si bien la relación asintótica (9) y el teoremaeTNP son equivalentes, no quiere decir que sean la misma cosa. En realidad, no todas las equivalencias asintóticas nacen iguales: el hecho aislado de saber que $a(x) \sim b(x)$ no nos dice demasiado acerca de la diferencia $|a(x) - b(x)|$. Dependiendo del caso, esa diferencia puede desde irse a cero, ser acotada o incluso crecer indefinidamente. El hecho de saber que se la diferencia se va a cero o a infinito, tampoco es suficiente para una descripión completa: queda abierta la importante cuestión sobre cuál es la velocidad en que lo hace. Ilustramos esto con un ejemplo muy sencillo: si se considera la función $a(x) = 3x^3 + 5x^2 + 4x + 4$, las funciones $b_1(x) = 3x^2 + 4x + 4$, $b_2(x) = 3x^2 + 5x^2 + 4$ y $b_3(x) = 3x^2 + 5x^2 + 4x$ son todas asintóticamente equivalentes con $a(x)$. Pero los términos de error en cada caso son muy distintos: $a(x) - b_1(x) = 5x^2$ y $a(x) - b_2(x) = 4x$ crecen ambas indefinidamente hacia infinio, pero la primera diferencia lo hace mucho más rápido. Por otro lado $a(x) - b_3(x) = 4$ es constante. Tenemos entonces la pregunta ¿Qué sucede en el caso del teorema de los números primos? Notemos primero que de (10) se sigue que la diferencia $\mathrm{Li}(x) - x/\log(x)$ es del orden $x/\log^2(x)$, que se va a infinito. Resulta ser que de entre las dos opciones $\mathrm{Li}(x)$ y $x/\log(x)$, la primera es una mejor aproximación para $\pi(x)$. De la Vallée–Poussin mostró que

$$|\mathrm{Li}(x) - \pi(x)| \leq Kxe^{-c\sqrt{\log(x)}}$$

para ciertas constantes positivas K y c. Las estimaciones de estas diferencias están fuertemente ligadas a tener regiones libres de ceros de la función zeta de Riemann fuera de la línea crítica. Si la hipótesis de Riemann resulta ser verdadera, entonces se tendría la cota óptima para la diferencia, que resulta ser

$$|\mathrm{Li}(x) - \pi(x)| \leq K\sqrt{x} \cdot \log(x)$$

para alguna constante K. Referimos a (Edwards, 2001) para demostraciones de las dos afirmaciones anteriores. Notemos que de esto se sigue que la aproximación de $\pi(x)$ por $\mathrm{Li}(x)$ es necesariamente mejor que la aproximación por $x/\log(x)$: en efecto, la diferencia entre $\mathrm{Li}(x)$ y $x/\log(x)$ es de orden de $x/(\log x)^2$, que es de orden mayor que el lado derecho de (4).

Previo a Riemann, los avances más importantes hacia una demostración del teorema de los números primos se atribuyen a Pafnuty Chebyshev. Estudiando la función zeta, aunque únicamente para valores reales de s, Chebyshev obtuvo resultados notables. Por una parte, demostró la cota

$$(0.89)\mathrm{Li}(x) \leq \pi(x) \leq (1.11)\mathrm{Li}(x).$$

Pr otra parte demostró que, en caso de existir, el límite de $\log(x)\pi(x)/x$ es necesariamente igual a 1 (Edwards, 2001). El trabajo de Chebyshev sobre la distribución de los números primos fue publicado en 1852 un par de artículos (Chebyshev, 1852a,b).

Como se mencionó, el teorema de los números primos fue demostrado originalmente usando técnicas de análisis complejo. Durante un tiempo, algunos matemáticos se preguntaron si era posible demostrar el resultado sin recurrir a esa poderosa herramienta teórica, usando únicamente métodos "elementales" de aritmética. La respuesta a esta pregunta resultó afirmativa: en 1949 Atle Selberg y Paul Erdös publicaron demostraciones elementales del teorema de los números primos (Selberg, 1949) y (Erdös, 1949). Cabe hacer mención que estas llamadas "demostraciones elementales" son en realidad mucho más elaboradas y complicadas en más de un sentido que las demostraciones basadas en teoría analítica de números. Para una discusión acerca de la historia de las demostraciones elementales del teorema de los números primos referimos a (Goldfeld, 2004).

MÁS ALLÁ DEL TEOREMA DE LOS NÚMEROS PRIMOS

Si bien el teorema de los números primos dice mucho acerca de la forma en que los números primos están distribuidos dentro de los enteros, deja sin resolver muchos misterios sobre los mismos. De hecho, pueden construirse conjuntos muy disímiles entre sí que satisfacen ese comportamiento asintótico. En esta sección comentaremos de forma breve acerca de algunas cuestiones en este sentido que han sido abordadas por algunos matemáticos en tiempos más recientes. Los resultados que mencionaremos en esta sección han sido obtenidos en su mayoría mediante técnicas muy sofisticadas de teoría analítica de números.

Para fijar ideas sobre lo que queremos decir, comenzaremos construyendo un par de conjuntos a los que llamaremos simplemente A y B, que serán muy distintos entre sí, pero ambos asintóticamente equivalentes al conjunto de los números primos. Para cada entero $n \geq 0$, denotemos por X_n al conjunto

$$X_0 = \{1\}, \qquad X_n = \{2^{n-1}+1, \ldots, 2^n\}.$$

Los conjuntos X_n así definidos son disjuntos a pares, su unión es todo $\mathbb{N}$ y para $n > 0$ el conjunto X_n tiene 2^{n-1} elementos (en particular, la cantidad de elementos de X_n crece exponencialmente con n). Observamos que el teorema de los números primos implica que el número de primos que hay dentro del conjunto X_n se aproxima asintóticamente a

$$\frac{2^n}{\log(2^n)} - \frac{2^{n-1}}{\log(2^{n-1})} = \frac{2^{n-1}}{n\log(2)}\left(2 - \frac{n}{(n-1)}\right) \tag{11}$$

$$= \frac{2^{n-1}}{n\log(2)}. \tag{12}$$

Sean A y B conjuntos tales que, en ambos casos, su número de elementos en cada X_n sea igual al entero más cercano a $2^{n-1}/n\log 2$ (llamémosle k_n), pero de forma que por un lado los elementos del conjunto A estén repartidos lo más uniformemente posible dentro de X_n, mientras que por otro lado los elementos de $B \cap X_n$ estén todos juntos.

Explícitamente,

$$A \cap X_n = \{2^{n-1}\left(1 + r\left\lfloor \frac{2^{n-1}}{k_n} \right\rfloor\right) \mid r = 0, \ldots, k_n\}.$$

$$B \cap X_n = \{2^{n-1}+1, \ldots, 2^{n-1}+k_n\}.$$

Estos dos conjuntos son bien distintos entre sí, pero ambos tienen comportamientos bastante regulares. Eso es a su vez muy distinto al comportamiento de los números primos que como se ha comentado es muy irregular. Sin embargo, los tres conjuntos en cuestión son asintóticamente equivalentes, y el teorema de los números primos no nos da información alguna para distinguir entre ellos. Podría decirse que el teorema de los números primos nos dice en cierto modo cuántos primos hay, pero nos dice muy poco acerca de dónde están.

Entre las líneas de investigación que pueden proponerse con el fin de entender mejor cómo se distribuye el conjunto de los números primos, una que tiene gran auge es el estudiar el tamaño de los espacios entre primos consecutivos. En concreto, esto puede plantrarse como el analizar el comportamiento de la función con valores enteros

$$g(n) = p_{n+1} - p_n,$$

donde p_n denota el n–ésimo número primo. Esta pregunta ha sido estudiada ampliamente desde principios del siglo XX, y hasta ahora solo se tienen algunas respuestas parciales. De hecho, ni siquiera el comportamiento asintótico de $g(n)$ ha podido ser determinado. Algo que sí se sabe es que la función $g(n)$ no es acotada. En otras palabras, para cualquier número entero M por grande que sea, existe una colección de M enteros consecutivos tales que ninguno de ellos es primo. Este hecho se sigue de forma inmediata del teorema de los números primos. En efecto, tenemos que para x grande, la distancia promedio entre primos consecutivos menores que x viene a ser aproximadamente igual a $\log(x)$. La distancia mayor debe superar a esa distancia promedio, y como la función logaritmo crece indefinidamente, dicha distancia no puede estar acotada.

En realidad, el teorema de los números primos es una herramienta demasiado poderosa para ver eso, ya que es posible verificar de forma muy sencilla y mediante métodos elementales el hecho de que existen espacios sin primos tan grandes como se quiera. Para M arbitrario, tómense los números

$$(M+1)!+2,\ (M+1)!+3,\ (M+1)!+4,\ \ldots,\ (M+1)!+(M+1).$$

Es claro que todos los elementos de esa lista son números compuestos, dado que $n!+k$ es múltiplo de k siempre que $k \leq M$. Así que tenemos M números consecutivos tal que ninguno de ellos es primo. Resalta de esta última construcción que los números que se toman son mucho más grandes que la longitud del intervalo M. Esto es, si bien la función

$$G(x) = \max_{p_n < x} g(n)$$

crece indefinidamente hacia infinito, parece hacerlo muy lentamente. En general, lo que se observa es que aunque el espacio entre primos consecutivos puede llegar a ser arbitrariamente grande, es siempre mucho más pequeño que el valor de los primos involucrados. Esto puede ya observarse empíricamente desde valores muy pequeños de n; por ejemplo, para los primos menores que 100, la mayor distancia entre primos consecutivos es 6, y para los primos menores que 1000 la mayor distancia es 20 (que ocurre entre 887 y 907). El estudio del comportamiento asintótico de la función G ha sio abordado con gran interés por matemáticos de renombre, y constituye un área de estudio de considerable actividad y producción en años recientes. En este sentido, una de las apuestas más significativas es demostrar (afirmativa o negativamente) la *conjetura de Cramer*. Esta conjetura, propuesta por el matemático sueco Harald Cramer (1936) establece que el crecimiento de la función $G(n)$ es de orden $\log^2(p_n)$, o de forma más precisa que existen constantes c_1 y c_2 tales que

$$c_1 \log^2(p_n) \leq G(p_n) \leq c_2 \log^2(p_n).$$

Una versión un tanto más fuerte de la conjetura de Cramer afirma que $G(x)$ es de hecho asintóticamente equivalente a $\log^2(x)$. Ninguna de las dos versiones ha sido ni demostrada ni rebatida hasta ahora. Se han

hecho considerables esfuerzos en esta dirección, tanto para acotar a $G(x)$ asintóticamente por arriba como por abajo. Entre las cotas superiores, el resultado más cercano a la conjetura de Cramer de la que tenemos noticia es que $G(x)$ es de orden no mayor que $x^{0.525}$ (Baker et al., 2001). Ya en su mismo artículo de 1936, Cramer había conseguido una cota algo mejor, al mostrar que el orden de $G(x)$ no excede a $\log(x)\sqrt{x}$; sin embargo, la prueba de Cramer depende de la veracidad de la hipótesis de Riemann. Desde luego, las dos cotas mencionadas están todavía muy lejos de la conjeturada por Cramer. En cuanto a cotas inferiores, la mejor de la que tenemos noticia fue la anunciada recientemente por Kevin Ford, Ben Green, Sergei Konyagin y Terence Tao (Ford et al., 2016) que establece la vistosa relación

$$G(x) \geq \frac{(\log x)(\log\log x)(\log\log\log\log x)}{\log\log\log x}.$$

Una nota curiosa e importante de observar acerca de la conjetura de Cramer es que fue motivada no tanto por el estudio del conjunto de los números primos como tal, sino del análisis de conjuntos aleatorios que son asintóticamente equivalentes al conjunto de los números primos. De manera más precisa, Cramer considera un conjunto en que para cada n se tira una moneda cargada con peso $n/\log(n)$ para decidir si está o no en el conjunto. El conjunto generado por este modelo estocástico original de Cramer puede incluso contener números consecutivos. Posteriormente se han estudiado versiones más refinadas de este modelo, evitando no solo parejas de números consecutivos, sino otras combinaciones de números que no pueden ocurrir dentro del conjunto de los números primos. La idea subyacente es que si bien el conjunto de los números primos es un conjunto determinista, parece tener una irregularidad propia de conjuntos aleatorios. A veces se usa el término "pseudoaleatorio" para describir el compartamiento de los números primos, y se espera que muchas de las propiedades de conjuntos generados aleatoriamente se reproduzcan también en el caso de los primos.

Como podemos observar, la pregunta anterior puede interpretarse como la búsqueda de espacios grandes entre primos. En sentido opuesto puede plantearse la cuestión de buscar espacios pequeños entre ellos. Esto resulta en preguntas que podemos considerar más intuitivas y que han atraído la imaginación de matemáticos de tiempos muy anteriores. Si bien en promedio los espacios entre primos crecen indefinidamente hacia infinito, esto no significa que no pueda haber una cota M finita tal que exista una infinidad de espacios entre primos consecutivos menores que M. El caso más extremo de esto, es una célebre conjetura conocida como la *conjetura de los primos gemelos*. Por primos gemelos se entiende una pareja de primos cuya diferencia es 2 (es decir, parejas de primos lo más cercanos posibles excepto por la pareja 2 y 3, ya que no hay otro primo par. Hay ocho parejas de primos gemelos menores que cien:

$$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (41,43),\ (59,61),\ (71,73).$$

La conjetura de los primos gemelos propone simplemente que existe una cantidad infinita de dichas parejas. No requiere un gran salto de imaginación suponer que dicha pregunta tan directa haya sido planteada desde la antigüedad, cosa que es creíble que pudiera cierta; sin embargo, la referencia publicada más antigua que se conoce es comparativamente muy reciente (De Polignac, 1849).

Conviene reformular la conjetura de los primos gemelos, introduciendo un poco de notación. Sea

$$h(n) = \min_{k\geq n}(p_{k+1} - p_k), \qquad H = \lim_{n\to\infty} h(n).$$

El límite H existe (aunque en principio pudiera ser infinito), puesto que la función h es monótona creciente. La conjetura de los primos gemelos corresponde a la afirmación $H = 2$, y es un problema que

permanece abierto a la fecha. Hasta hace poco no se sabía ni siquiera si el valor de esta H era finito. La finitud de H fue verificada afirmativamente por Yitang Zhang (2014), quien consiguió mostrar que el valor de H es menor que 70 millones. Este resultado es considerado de magnitudes históricas, y sin duda uno de los resultados más importantes en teoría de números de las últimas décadas; un aspecto muy curioso es que al momento de anunciar el resultado, Zhang era un matemático muy poco conocido y contaba ya con 58 años de edad (Klarreich, 2014). A partir de este resultado, muchos expertos en el problema se han dado a la tarea de reducir la cota para valores posibles de H. Muchos de los esfuerzos más importantes se han concentrado en el proyecto Polymath8. Los proyectos Polymath son una novedosa forma de hacer investigación en matemáticas, muy acorde a nuestros tiempos: en un blog en internet se propone un problema abierto y se invita a la comunidad matemática mundial a resolverlo. La idea es crear una especie de colaboración masiva para resolver problemas. Los resultados obtenidos se publican bajo el pseudónimo D.H.J. Polymath. El proyecto Polymath8 se separó en dos etapas: en la primera se refinaron las técnicas usadas por Zhang, lográndose reducir la cota para H a 4,680 (Polymath, 2014a; Castryck et al., 2014). En la segunda se usaron técnicas atribuidas al joven matemático británico James Maynard (nacido en 1987 y uno de los principales expertos de la actualidad en el estudio de espacios entre primos). Con estas técnicas se logró reducir la cota para H a 246 (Polymath, 2014b).

Otro resultado reciente de considerable importancia en la materia, es el teorema de Green–Tao, referente a progresiones aritméticas de primos (Green and Tao, 2008). Una progresión aritmética no es más que una lista de números tal que la distancia entre cualesquiera dos números consecutivos de la lista es siempre la misma. Por ejemplo la secuencia

$$7,\ 37,\ 67,\ 97,\ 127, 157$$

es una progresión aritmética formada por seis primos, en que la distancia entre ellos aumenta de treinta en treinta. Notemos que en una progresión aritmética de cinco o más elementos, para que sean todos primos es necesario que la distancia entre ellos sea múltiplo de 2, 3 y 5, o sea que debe ser al menos 30. De la misma forma, para poder agregar un séptimo primo la distancia entre ellos debe aumentar en un múltiplo de 210. El teorema de Green–Tao dice que para todo entero positivo k, por grande que sea, existe una infinidad de progresiones aritméticas de longitud al menos k que están formadas exclusivamente por números primos. Antes de haberse probado este teorema, no se sabía ni siquiera si había una infinidad de progresiones aritméticas de primos con cuatro elementos. El resultado para $k = 3$ era lo mejor que se tenía, y había sido establecidoya muchos años antes (Van der Corput, 1939).

Como hemos visto en repetidas ocasiones, la distribución de los números primos ha sido fuente de muchas conjeturas, algunas de las cuales se han demostrado y otras permanecen abiertas. De entre estas conjeturas hay una que ocupa un lugar primordial: la llamada *primera conjetura de Hardy–Littlewood*, que concierne a las llamadas *constelaciones de primos* y que fue enunciada en (Hardy and Littlewod, 1923). Lo sobresaliente de esta conjetura es que establece con extremada precisión la forma en que estarían distribuidos asintóticamente los números primos. Por constelación de primos nos referimos a grupos de primos consecutivos que siguen un patrón establecido de la forma

$$p, p+2k_1, p+2k_2, \ldots, p+2k_r \tag{13}$$

para alguna elección de enteros $k_1 < k_2 < \cdots < k_r$. Por ejemplo, cuando se tiene $r = 1$ y $k_1 = 1$ se tienen primos gemelos. Puede decirse que los primos gemelos son el ejemplo más sencillo de constelación de primos. Constelaciones con tres elementos y correspondientes a $k_1 = 1, k_2 = 3$ serían por ejemplo las ternas $(17, 19, 23)$ y $(41, 43, 47)$. Un concepto importante a tener en cuenta cuando hablamos de constelaciones de primos es la de que la colección de enteros $\{k_1, \ldots, k_r\}$ sea o no un *patrón admisible*: si

dicha colección contiene todos los residuos no cero posibles módulo q para algún primo q (necesariamente menor que r), uno de los números en (13) sería múltiplo de q y por lo tanto ninguna constelación asociada a ese patrón podría estar formada exclusivamente números primos, a menos que uno de ellos fuera precisamente q. En particular, en ese caso hay a lo más una cantidad finita de constelaciones de primos asociadas al patrón, y se dice que el patrón es no admisible. En caso contrario, se dice que la colección es admisible. El ejemplo más sencillo de colección no admisible es la que se obtiene al tomar $k_1 = 1, k_2 = 2$; es decir ternas de la forma $a, a+2, a+4$. En dichas ternas uno de los tres números es múltiplo de 3, por lo que la única constelación de primos que le corresponde es la terna $(3,5,7)$. En resumen, hay patrones admisibles y no admisibles; para estos últimos puede haber a lo mucho una constelación. Para los patrones admisibles, podría haber infinitas constelaciones, pero ¿cuántas hay en realidad? En general no se sabe. Se conocen patrones admisibles explícitos para los cuales no se sabe a ciencia cierta ni siquiera si hay una constelación de primos. La conjetura de Hardy–Littlewood arriba anunciada nos que hay una infinidad de constelaciones de primos para todos y cada uno de los patrones admisibles. La conjetura de los primos gemelos viene a ser, desde luego, un caso particular. En realidad la conjetura de Hardy–Littlewood dice muchísimo más: nos da una fórmula asintótica para la distribución asintótica de la constelación, y lo hace en el espíritu del teorema de los números primos.

En concreto, de acuerdo a dicha conjetura, si denotamos por $\pi_k(x)$ al número de constelaciones (13) para el patrón $k = \{k_1, \ldots, k_r\}$ tales que $p < x$, entonces

$$\pi_k(x) \sim C_k \int_2^\infty \frac{dt}{[\log(t)]^r}$$

para cierta constante C_k que depende del patrón k y que Hardy y Littlewood expresan de manera explícita. Esta conjetura es usualmente considerada como cierta, y existe una cantidad considerable de evidencia sobre su veracidad. Sin embargo, a la fecha el resultado parece todavía estar muy lejos de ser demostrado.

Existe una segunda conjetura de Hardy y Littlewood que fue propuesta en el mismo artículo (Hardy and Littlewod, 1923), que si bien no hace una descripción tan explícita tiene la virtud de ser muy natural, intuitiva y simple. Lo que dice esta segunda conjetura es que

$$\pi(n+m) - \pi(n) \leq \pi(m) \tag{14}$$

para todos los valores de n y m. En otras palabras, si tomamos una colección de m números consecutivos, entre ellos no puede haber más primos que los que hay entre los primeros m enteros. Por ejemplo, hay 25 primos entre los números menores que 100, de modo que la segunda conjetura de Hardy y Littlewood nos asegura que no puede haber más de 25 primos en ninguna otra lista de cien números consecutivos. Esto es desde luego de esperarse, puesto que el conjunto de los números primos se va haciendo cada vez más disperso conforme nos alejamos hacia infinito (es lo que nos dice no solo la observación empírica, sino también el teorema de los números primos). Además de esto, los cálculos numéricos que se han hecho de $\pi(x)$ (que, gracias al poder de cómputo electrónico ahora disponible, ha podido hacerse para valores muy grandes de x) no han arrojado ningún ejemplo que contradiga la conjetura. Sin embargo, en Hensley and Richards (1974) se demostró que las dos conjeturas de Hardy y Littlewood no pueden ser ambas ciertas: si la primera es verdadera, entonces la segunda tiene que ser falsa y viceversa. Nos encontramos entonces con dos situaciones en principio muy plausibles acerca de los números primos, de las cuales al menos una (o tal vez ambas) es falsa. La interesante historia de cómo llegaron a ese resultado está contada de manera un tanto informal en (Richards, 1974).

Lo que Hensley y Richards demostraron es que si m es suficientemente grande (sin pérdida de generalidad suponemos que m es par con $m = 2s$), entonces existe un patrón admisible $k_1, \ldots k_r = s$ con

$r+1 > \pi(m)$. Es decir, probaron que existe un patrón contenido en un intervalo de longitud x que tiene más elementos que el número de primos menores o iguales a n. Entonces, si la primera conjetura de Hardy – Littlewood fuese verdadera, para ese patrón existiría una cantidad infinita de constelaciones de primos para ese patrón y todas ellas estarían contenidas en un intervalo de longitud m, pero tendrían más de $\pi(m)$ elementos. Esto es, la veracidad de la primera conujetura no solamente contradice (14) sino que lo hace para infinitos valores de n.

De hecho, si la primera conjetura de Hardy–Littlewood es verdadera, entonces:

1. La segunda conjetura falla para todos los valores de m suficientemente grandes.
2. Y para cada uno de esos m falla infinitas veces.

Como se puede observar, la primera conjetura parece ser una herramienta demasiado poderosa para rebatir la segunda conjetura. Sería suficiente demostrar que para una sola de los patrones admisibles largos mencionados arriba existe una contelación de primos asociada. Esto parece sin duda mucho más sencillo que demostrar la primera conjetura, e incluso podría parecer tentador usar computadoras para encontrar numéricamente una constelación de ese tipo. Sin embargo, el tamaño de los primos que estarían involucrados es demasiado grande para el poder de cómputo existente en la actualidad. La existencia de una de esas constelaciones de primos tampoco se ha podido demostrar por medios teóricos. El pregunta sobre cuál de las conjeturas es cierta sigue en el aire, mientras que la incompatibilidad entre ellas prevalece como uno más de los profundos misterios con los que nos encontramos al analizar la forma en que los números primos están distribuidos dentro de los enteros.

REFERENCIAS

Apostol, T. (1998). *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. Springer.

Apostol, T. (2001). The most surprising result in mathematics. *The Mathematical Intelligencer*, pages 1–26.

Apéry, R. (1979). Irrationalité de $\zeta(2)$ et $\zeta(3)$. *Asterisque*, 61:11–13.

Baker, R., Harman, G., and Pintze, J. (2001). The difference between consecutive primes. II. *Proc. London Math. Soc. (3)*, 83(3):532–562.

Barlow, M. and Taylor, S. J. (1989). Fractional dimension of sets in discrete spaces. *J. Phys A: Math. Gen*, 22:2621–2626.

Barrera Fragoso, I. and Rojas Chavarría, R. G. (2017). El problema de Basilea. *Padi*, 5(8).

Castryck, W., Fouvry, E., Harcos, G., Kowalski, E., Michel, P., Nelson, P., Paldi, E., Pintz, J., Sutherland, A., Tao, T., and Xie, X. (2014). New equidistribution estimates of Zhang type. *Algebra and Number Theory*, 8(9):2067–2199.

Chebyshev, P. (1852a). Mémoire sur les nombres premiers. *J. Math. Pures Appl.*, 27:366–390.

Chebyshev, P. (1852b). Sur la fonction qui détermine la totalité des nombres premiers inférieurs à une limite donnée. *J. Math. Pures Appl.*, 27:341–365.

CMI (2000). Recent Diophantine results on zeta values: a survey. En http://www.claymath.org/millennium-problems.

Cramer, H. (1936). On the order of magnitude of the difference between consecutive prime numbers. *Acta Arithmetica*, 2:23–46.

De la Vallée Poussin, C.-J. (1896). Recherches analytiques sur la theorie des nombres: Premier partie: La fonction $\zeta(s)$ de Riemann et les nombres premiers en general. *Annales de la Soc. scientifique de Bruxelles*, 20:183–256.

De Polignac, A. (1849). Recherches nouvelles sur les nombres premiers. *Comptes Rendus des Séances de l'Académie des Sciences*.

Edwards, H. (2001). *Riemann Zeta Function*. Dover Publications Inc.

Erdös, P. (1949). On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. *Proc. Nat. Acad. Scis. U.S.A.*, 35:374–384.

Euclides (2005). *Elementos. Libros V–IX*. Traducción de María Puertas–Castaños. Biblioteca Clásica Gredos.

Euler, L. (1737). Variae observations circa series infinitas. *Comentarii academiar scientarum Petropolitanae*, 9(1744):160–188.

Fine, B. and Rosenberger, G. (2010). An epic drama: the development of the prime number theorem. *SCIENTIA, Series A: Mathematical Sciences*, 20:1–26.

Ford, K., Green, B., Konyagin, S., Maynard, J., and Tao, T. (2016). Long gaps between primes. *arXiv:1412.5029v3 [math.NT]*.

Goldfeld, D. (2004). The elementary proof of the prime number theorem: an historical perspective. In *Number Theory*. Springer.

Grabinsky, G. (2007). Euler, el prestidigitador de las series. *Miscelánea Matemática*, 45:55–66.

Green, B. and Tao, T. (2008). The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics*, 167(2).

Grey, J. (2015). *The Real and the Complex: A History of Analysis in the 19th Century*. Springer Undergraduate Series. Springer.

Hadamard, J. (1896). Sur la distribution des zeros de la fonction $\zeta(s)$ et ses consequences arithmetiques. *Bull. de la Soc. Math, de France*, 24:199–220.

Hardy, G. and Littlewod, J. (1923). Some problems of 'Partitio Numerorum.' III. on the expression of a number as a sum of primes. *Acta Math.*, 44:1–70.

Hensley, D. and Richards, I. (1974). Primes in intervals. *Acta Arith.*, 25:375–391.

Hilbert, D. (1902). Mathematical problems. *Bull. Amer. Math. Soc.*, 8(10).

Klarreich, E. (2014). Unheralded mathematician bridges the prime gap. *Annals of Mathematics*, 1121-1174.

Polymath, D. (2014a). New equidistribution estimates of Zhang type. *arXiv:1402.0811v3 [math.NT]*.

Polymath, D. (2014b). Variants of the Selberg sieve, and bounded intervals containing many primes. *Mathematical Sciences*, page 1:12.

Richards, I. (1974). On the incompatibility of two conjectures concerning primes; a discussion of the use of computers in attacking a theoretical problem. *Bull. Amer. Math. Soc.*, 80(3).

Riemann, B. (1859). Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsberichte der Berliner Akademie*.

Selberg, A. (1949). An elementary proof of the prime-number theorem. *Annals of Mathematics.*, 50 (2):305–313.

Sánchez Muñoz, J. (2014). El problema de Basilea. *Lecturas Matemáticas*, 35(2):199–228.

Van der Corput, J. (1939). Uber Summen von Primzahlen und Primzahlquadraten. *Math. Ann.*, 116:1–50.

Waldschmidt, M. (2009). Recent Diophantine results on zeta values: a survey. En https://webusers.imj-prg.fr/ michel.waldschmidt/articles/pdf/MZV2011IMSc.pdf.

Zhang, Y. (2014). Bounded gaps between primes. *Annals of Mathematics*, 1121-1174.

[1]Profesor investigador del Área Académica de Matemáticas y Física