DIOS SALVE A LA REINA[1]

La matemática es la reina de las ciencias y la teoría de números es la reina de la matemática. Carl F. Gauss

Introducción

En este artículo presentaremos algunas ideas de aquella rama de la matemática capaz de motivar la exaltada manifestación del epígrafe, proveniente nada menos que del más importante matemático de todos los tiempos. Nos referimos a la teoría de números, que cautiva tanto a matemáticos profesionales como a legos, en cuyo marco se plantearon problemas que aún hoy desafían a las mentes más poderosas.

Al margen de su innegable belleza, una de las razones del interés que despierta consiste en que su materia es elemental, aunque constituye el fundamento de la matemática: los números naturales. Los problemas que trata la teoría de números, también llamada aritmética, involucran únicamente a los números enteros positivos y las operaciones básicas: por ejemplo, puede ser un problema el de estudiar las soluciones enteras de una ecuación diofántica, o la descomposición de un número en sus factores primos. Pero el hecho de que su "materia" sea elemental no significa que lo sean sus procedimientos o sus métodos, que a menudo recurren a otras ramas de la matemática: por el contrario, muchos de los problemas más complicados de los últimos siglos provienen de la teoría de números y pueden ser planteados en los términos más sencillos.

En las páginas que siguen describiremos algunos de tales problemas, cuya historia está colmada de éxitos pero también de resonantes fracasos.

El artículo está organizado de la siguiente forma:

La segunda sección está dedicada a uno de los teoremas fundamentales de la teoría de números, anunciado por Fermat en 1636 aunque fue probado (y generalizado) algunas décadas más tarde por Euler. En la sección siguiente haremos referencia a otro teorema de Fermat, no tan importante pero sí extraordinariamente famoso a causa de la larga epopeya que significó su demostración. Finalmente, en las últimas secciones nos ocuparemos de enunciar con bastante cuidado la no menos famosa conjetura conocida como *Hipótesis de Riemann*, que sin duda se encuentra entre los más apasionantes -y difíciles- problemas jamás planteados.

Cartas a un joven matemático

En el siglo XVII, un abogado francés pasaría a la historia como uno de los más grandes matemáticos de todos los tiempos. Se trata de Pierre de Fermat, de quien se conocen numerosos resultados que solía anunciar a través de cartas que enviaba a sus amigos. En una de ellas, destinada a otro matemático francés llamado Frénicle de Bessy, presentó un hecho que revela una propiedad magnífica de los números primos, que son aquellos números mayores que 1 solo divisibles por sí mismos y por la unidad:

> Si n es un número primo y a es otro número cualquiera, entonces el resto de dividir a^n por n y el de dividir a por n es exactamente el mismo.

A modo de ejemplo sencillo, tomemos $n = 3$ y $a = 215$: haciendo la cuenta, 215 dividido 3 es 71, y el resto es 2, mientras que $215^3 = 9938375$, que dividido por 3 da 3312791, y el resto también es 2.

---

[1] Artículo publicado en el libro *Viaje a la Complejidad. Vol 1: Del Big Bang al origen de la vida.* Nicolás Caparrós y Rafael Cruz Roche (dirs.). Ed. Biblioteca Nueva, Madrid 2012.

Por cierto, la gracia del teorema consiste en que permite conocer el resto sin necesidad, justamente, de “hacer la cuenta”: por ejemplo, podemos afirmar con toda tranquilidad que el resto de dividir 40^{29} es 11, sin que haga falta pasar un buen rato ocupados en tediosos cálculos. Tan asombrosa propiedad ha motivado en los últimos tiempos una aplicación muy interesante y útil en aquella técnica destinada a codificar mensajes que recibe el nombre de *criptografía*.

Vale la pena mencionar que el enunciado original era ligeramente diferente: en su carta, Fermat decía que

> *...todo número primo n divide a los términos de una progresión en los que el exponente es un múltiplo de n, menos uno.*

Esta forma de enunciarlo no es del todo clara, pero expresa el hecho de que cualquier número de la forma $a^{k(n-1)} - 1$ es múltiplo de n. En realidad, hace falta pedir también que a no sea múltiplo de n; una vez aclarado este detalle, es fácil ver que el enunciado equivale al anterior. Por ejemplo, si tomamos como antes $n = 3$ y $a = 215$, para $k = 1$ obtenemos

$$215^2 - 1 = 46224,$$

que es múltiplo de 3.

Más allá del valor de este hallazgo, merece un comentario aparte una curiosa frase que escribió Fermat en su misiva, a continuación del teorema:

> *Y esta proposición es generalmente cierta para todas las progresiones y todos los números primos; le enviaría la prueba, si no temiese que es demasiado larga.*

La excusa podría resultar aceptable si Fermat hubiese intentado comunicar su teorema por algún medio más precario como *Twitter* o enviando un *sms*; cuesta pensar que la carta fuera a resultar mucho más abultada por el simple hecho de contener la demostración. Claro que esto no es del todo cierto, como lo justifican infinidad de demostraciones muy largas y complejas de otros resultados matemáticos; sin embargo, en este caso, es posible encontrar una prueba que solo necesita de unos pocos renglones, al menos si se escribe con letra apretada.

Por ejemplo, ello ocurre con la demostración que publicó un siglo más tarde el prolífico matemático suizo Leonhard Euler, años antes de quedar completamente ciego. En rigor, la misma prueba había sido hallada por otro notable genio, el alemán Gottfried Leibniz: haciendo uso de aquella propiedad básica de los números naturales denominada *principio de inducción*, es muy fácil ver que la afirmación de que el primo n divide a la cantidad $a^n - a$ es válida para todo a.[2]

Pero los trabajos de Euler permitieron encontrar una generalización realmente sorprendente del teorema original, que ya no se restringe a los primos sino que vale para cualquier número natural n, siempre que a y n no tengan divisores comunes mayores que 1 (vale decir, que sean *coprimos*, o primos entre sí). El enunciado requiere una nueva definición, aunque muy fácil de entender: se trata de la *función de Euler*, denotada por medio de la letra griega φ, que para cada n se define como la cantidad de números menores que n que no tienen divisores comunes con él. Por ejemplo, para el número 8 hay cuatro números menores que 8 y coprimos con él: 1, 3, 5 y 7: de esta forma, $\varphi(8) = 4$. Como ejercicio, el lector puede calcular los valores de φ para algunos otros casos, por ejemplo:

$$\varphi(12) = 4,$$

$$\varphi(28) = 12,$$

$$\varphi(32) = 16.$$

[2] Para el lector interesado en reproducir dicha prueba, vale la pena observar que, empleando el desarrollo del *binomio de Newton* y el hecho de que n es primo se verifica que $(a + 1)^n - (a^n + 1)$ es múltiplo de n. A partir de allí, el resultado se sigue de forma inmediata.

El teorema probado por Euler (también llamado *de Euler-Fermat*) dice que para cualquier n y cualquier a coprimo con n vale que $a^{\varphi(n)} - 1$ es múltiplo de n.

A modo de ejemplo, consideremos $n = 28$. Los números coprimos con 8 son los impares que además no son múltiplos de 7, y como $\varphi(28) = 12$ entonces el teorema asegura que $a^{12} - 1$ tiene que ser múltiplo de 28.

Como caso particular, es claro que si n es un número primo entonces $\varphi(n)$ es $n - 1$, lo que restablece el enunciado original de Fermat (con $k = 1$).

El Fermat grande se come al chico

El resultado que vimos en la sección previa para el caso particular de los números primos se conoce habitualmente como *pequeño teorema de Fermat*; no porque en verdad lo sea, sino más bien para diferenciarlo de ese otro cuya historia lo ha hecho "grande". Se trata del denominado *último teorema*, que ha terminado de probarse hace menos de dos décadas. Su enunciado original, de 1637, no aparece en una carta sino en el margen de un libro (la *Arithmetica* de Diofanto), lo que justifica un poco mejor que antes la nueva omisión:

> *He encontrado una demostración realmente admirable, pero el margen de este libro es muy estrecho para contenerla.*

A esta altura deberíamos pensar que Fermat tenía cierta manía de dejar los teoremas sin demostración. Esto es cierto en buena medida, aunque en la mayoría de los casos las pruebas que no llegó a escribir fueron completadas muy pronto por otros autores. El "último teorema", en cambio, debió esperar más de tres siglos de idas y venidas hasta que en 1994 un matemático inglés llamado Andrew Wiles logró establecer los últimos detalles de la prueba, que comprende un centenar de páginas y recorre varias ramas de la matemática. Lo curioso es que la propiedad en sí es sencilla, más bien insignificante; se trata de una propiedad de los números enteros sin mayores consecuencias visibles: para cualquier entero n mayor que 2, la ecuación

$$a^n + b^n = c^n$$

no tiene soluciones enteras. Justamente a raíz de su "sencillez" es que se la ha presentado como un ejemplo paradigmático de ese antiguo ideal que dice que un problema matemático es bueno solamente cuando se lo puede explicar a la primera persona que encontremos en la calle. Claro que la resolución, en este caso, ha demandado un esfuerzo más que considerable y dista mucho de satisfacer dicho ideal, a menos que tengamos la extraordinaria suerte de que la primera persona que encontremos en la calle sea uno de los poquísimos individuos en el mundo capaces de comprender la demostración de Wiles[3].

Mucho se ha escrito sobre este problema y su curiosa historia, cuya versión más romántica incluye desengaños amorosos e intentos de suicidio -uno de ellos exitoso, si se lo puede llamar así- aunque tiene un final feliz.[4]

---

[3] Para dar una idea más precisa de esto, diré que aun siendo matemático debería dedicar un buen tiempo solamente para estudiar algunas de las teorías que se requieren para entender dicha demostración. De este modo, si al salir a la calle me encontrara con alguien dispuesto a explicarme el último teorema de Fermat con todo rigor, recién podría volver a casa al cabo de algunos años.

[4] Algunas de estas anécdotas se cuentan en mis libros *La matemática como una de las bellas artes* y *¡Matemática, maestro! Un concierto para números y orquesta*, ambos publicados por Siglo XXI. Pero existen diversos textos dedicados específicamente al teorema y su demostración. Uno de los más conocidos, destinado al público no matemático, es el de Simon Singh: *El último*

A mar revuelto, problema no resuelto

Un año allá por la década de 1930, terminaba el verano en Dinamarca y el matemático inglés George Hardy debía retornar a casa para comenzar sus clases. Había pasado unos meses visitando a Harald Bohr, hermano del conocido físico. El asunto es que solo había un barco disponible para la travesía, que era amenazadoramente pequeño como para atravesar las aguas a menudo inquietas del Mar del Norte. Hardy emprendió el viaje, aunque antes de hacerlo envió a Bohr una postal que decía:

He probado la Hipótesis de Riemann.

G. H. Hardy.

La anécdota es referida por otro famoso matemático del siglo XX, el húngaro George Pólya, quien explica las razones de tan curioso mensaje de la siguiente manera: *Si el bote se hundía y Hardy se ahogaba, todo el mundo creería que él había probado la Hipótesis de Riemann. Pero Dios no consentiría que él (Hardy) tuviera ese gran honor y por esto no iba a dejar que el bote se hundiera.*

Es justo reconocer que el ardid es, cuanto menos, una forma muy original de cubrirse contra los riesgos de hacerse a la mar. El bote, en efecto, no se hundió y la Hipótesis de Riemann sigue siendo uno de los grandes problemas no resueltos de la matemática.

Pero no fue Hardy el único interesado en tales asuntos: otra anécdota cuenta que a Hilbert, el más grande matemático del siglo XX, le pidieron una vez que dijera qué haría en caso de volver a la vida al cabo de algunos siglos. El alemán respondió que lo primero sería preguntar: ¿Ha probado alguien la hipótesis de Riemann?

A la luz de estas historias, vale la pena conocer más de cerca tan notable problema, capaz de obsesionar a tan notables personajes. A diferencia del último teorema de Fermat, la hipótesis de Riemann figura en la famosa lista de los 23 problemas no resueltos que presentó Hilbert en 1900. Un siglo más tarde, el Clay Mathematics Institute publicaría una lista análoga pero ahora de 7 problemas, conocidos como “los problemas del milenio”, con el incentivo adicional (al menos para muchos) de un suculento premio de un millón de dólares para quien fuera capaz de resolver cualquiera de ellos. En la lista aparece, una vez más, la hipótesis de Riemann.

La conjetura fue formulada por el matemático alemán Bernhard Riemann en 1859, en un artículo de 8 páginas que presentó luego de ser admitido como miembro de la Academia de Berlín, titulado *Sobre el número de primos menores que una cantidad dada.* El asunto, pues, tiene que ver con los números primos, aunque la hipótesis de Riemann no se refiere a ellos sino a una función llamada *zeta* (ζ):

Todos los ceros no triviales de la función zeta tienen parte real igual a 1/2.

Este breve enunciado deja ver a las claras otra diferencia crucial con el último teorema de Fermat: parece más bien difícil que “el hombre de la calle” logre entender de qué se trata sin unas cuantas explicaciones previas. En efecto, más allá de las dificultades que aún persisten para encontrar su resolución, el simple hecho de intentar comprenderla nos obliga a meternos en diversos temas de la matemática, que van desde el análisis, las series y los productos infinitos hasta los números complejos. Las próximas páginas estarán dedicadas a desarrollar algunos de estos temas.

---

teorema de Fermat, de atractiva lectura aunque contiene algunas inexactitudes. Muchas de ellas, de origen histórico, se señalan en el interesante artículo de Leo Corry, *El teorema de Fermat y sus historias*, La Gaceta de la Real Sociedad Matemática Española, Vol. 9, 2 (2006), 387–424, que contribuye en buena medida a desmitificar ciertos aspectos del famoso teorema.

...el objetivo inmediato de mi investigación

Antes de introducirnos en el problema en cuestión, vale la pena mencionar que el artículo original de Riemann buscaba en realidad responder una pregunta básica: dado un número *n*, ¿cuántos primos menores que *n* hay? Por ejemplo, si *n* es 30 entonces hay diez: 2, 3, 5, 7, 11, 13, 17, 19, 23 y 29. Si *n* es 40, se agregan el 31 y el 37, de modo que en total hay doce. En general, esto no es algo que se pueda saber con exactitud para un número dado cualquiera, aunque es claro que se hace más grande a medida que *n* crece. Para estudiar este problema, Riemann definió un llamativo objeto que es la función zeta, y en las primeras páginas del artículo deslizó un comentario incidental, que se transformaría en la famosa "hipótesis". En verdad, se trata de una conjetura; según las propias palabras del autor:

> *A uno le gustaría, por cierto, tener una prueba rigurosa de esto, pero he dejado de lado la búsqueda de tal prueba al cabo de unos intentos rápidos y vanos, porque no es necesaria para el objetivo inmediato de mi investigación.*

Cabe destacar que el comentario resultó muy atinado, puesto que el "objetivo inmediato" de tal investigación alcanzó uno de sus puntos culminantes en un notable teorema demostrado en 1896 en forma casi simultánea por Jacques Hadamard y Charles de la Vallée Pousin: el *teorema de los números primos*. La prueba emplea un resultado que guarda conexión cercana con la hipótesis de Riemann, pero es más débil y pudo ser comprobado en forma directa. Más de un siglo después, la pregunta sobre la veracidad de la conjetura de Riemann permanece aún sin respuesta.

Veamos en qué consiste el teorema probado por estos dos destacados matemáticos, uno francés y el otro belga. Según hemos mencionado, Riemann se preguntó por la cantidad de primos menores que un número *n* dado; cuando escribió su artículo, el teorema de los números primos ya existía en forma de conjetura desde hacía unos cincuenta años. A grandes rasgos, su enunciado dice que la cantidad de primos menores que *n* se asemeja, cuando *n* es grande, a la función $n/\log(n)$, en donde "log" representa el famoso logaritmo (en base *e*) de una cantidad dada.

Conviene aclarar un poco más lo que significa eso de "asemejarse", para lo cual vale la pena construir una sencilla tabla. En la primera columna se indican los valores de *n*, cada vez más grandes; en la segunda, la cantidad de primos menores que dicho *n*, habitualmente denotada $\pi(n)$. Finalmente, la tercera columna indica el resultado de dividir *n* por su logaritmo:

n	$\pi(n)$	$n/log(n)$
1000	168	144,7648…
1000000	78498	72382,41365…
1000000000	50847534	48254942,43369…
1000000000000	37607912018	36191206825,2709…
1000000000000000	29844570422669	28952965460216,7885…
1000000000000000000	24739954287740860	24127471216847323,758…

Se observa entonces un nítido "parentesco", que no es *absoluto* sino *relativo*. Por ejemplo, si uno resta los dos valores del último renglón el resultado es muy grande:

$$24739954287740860 - 24127471216847323{,}758\ldots = 612483070893536{,}241\ldots$$

Sin embargo, se trata de una diferencia insignificante cuando se la compara con las enormes cantidades que estamos restando. Una forma de convencerse de esto consiste simplemente en efectuar el cociente, y verificar que da un resultado bastante cercano a 1:

$$24739954287740860/24127471216847323{,}758\ldots = 1{,}025\ldots$$

Otra manera muy sugestiva de expresar el teorema consiste en decir que la probabilidad de que un número elegido al azar entre los *n* primeros sea primo es, para *n* grande, aproximadamente $1/\log(n)$. Este valor tiende a cero, lo que significa que los primos se hacen cada vez más escasos a medida que tomamos "tiras" de números naturales cada vez más largas.[5]

La hipótesis de Riemann, de la A a la ζ

En las páginas que siguen presentaremos por fin la célebre función zeta de Riemann, lo que constituye un paso crucial a la hora de comprender el enunciado de su no menos célebre conjetura. Según hemos mencionado, para poder llevar a cabo tal empresa nos veremos en la necesidad de introducirnos en algunos otros temas, que comienzan con el análisis matemático y las series infinitas. Esto le da un sentido cabal al título de la sección, en donde la ζ remite obviamente a la zeta, mientras que la A puede pensarse a su vez como la inicial de una de las más importantes series matemáticas, la denominada *serie armónica*. Como veremos, de alguna manera es posible decir, en este contexto: *en el comienzo fue la Armónica*.

En principio, conviene precisar un poco el concepto de serie, con frecuencia mal entendida como una "suma infinita", que suele escribirse de la siguiente forma:

$$\sum_{n=1}^{\infty} a_n = a_1 + a_2 + a_3 + a_4 + \ldots$$

Pero en realidad no se trata de una suma sino de un *límite,* el límite de la suma de los primeros *N* términos, cuando *N* tiende a infinito. Por ejemplo, es una serie aquella que casi siempre se menciona cuando se habla de las aporías de Zenon, y aparece también en la literatura, tanto en Kafka como en Borges:

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\ldots=1$$

El hecho es que el resultado 1 no se obtiene "sumando infinitos términos" sino, como anticipamos, a partir del cálculo del límite de la sucesión formada por las denominadas *sumas parciales*:

$$S_1 = \frac{1}{2}$$

$$S_2 = \frac{1}{2}+\frac{1}{4}=\frac{3}{4}$$

$$S_3 = \frac{1}{2}+\frac{1}{4}+\frac{1}{8}=\frac{7}{8}$$

El lector más o menos avezado podrá intuir ya una fórmula general para calcular el valor exacto de S_N para este caso, y con un pequeño esfuerzo adicional será capaz también de demostrarla. Para dar una prueba apenas diferente de la convencional, podemos observar el simple hecho de que

$$\frac{1}{2^N}+\frac{1}{2^N}=\frac{2}{2^N}=\frac{1}{2^{N-1}}$$

[5] Cabe aclarar que el teorema ha sido objeto de sucesivas mejoras en lo que respecta a establecer con precisión la forma en que se "asemejan" las cantidades $\pi(n)$ y $n/\log(n)$. En particular, si se lograra probar la hipótesis de Riemann, entonces se obtendría una expresión muy exacta para acotar la diferencia entre una y otra.

y entonces vale:

$$S_N+\frac{1}{2^N}=\frac{1}{2}+\ldots+\frac{1}{2^{N-1}}+\frac{1}{2^N}+\frac{1}{2^N}=S_{N-1}+\frac{1}{2^{N-1}}.$$

En consecuencia, por un argumento inductivo verificamos que

$$S_N+\frac{1}{2^N}=S_{N-1}+\frac{1}{2^{N-1}}=\ldots=S_1+\frac{1}{2^1}=1,$$

de donde se deduce finalmente la fórmula:

$$S_N=1-\frac{1}{2^N}=\frac{2^N-1}{2^N}.$$

Pero más que la fórmula en sí, lo que interesa aquí es observar que su valor converge a 1; vale decir, las sumas parciales se aproximan cada vez más a 1 a medida que N tiende a infinito. Eso autoriza a escribir el "=" en la expresión

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\ldots=1,$$

que -aunque a veces sorprenda- no quiere decir que los dos términos "se parecen" sino que se trata de una igualdad hecha y derecha. La justificación proviene de la definición precisa y nada esotérica del concepto de límite.[6]

La serie armónica, en cambio, no es convergente sino que *diverge*, pues sus valores se hacen cada vez mayores a medida que N crece, sin que haya un "techo" o, mejor dicho, una cota[7]. El término general de esta nueva serie es $a_n = 1/n$, de modo que las sucesivas sumas parciales son:

$$S_1 = 1$$

$$S_2=1+\frac{1}{2}=\frac{3}{2}$$

$$S_3=1+\frac{1}{2}+\frac{1}{3}=\frac{11}{6}$$

...

[6] Una manera inmediata de reforzar este concepto es a partir de la idea, muy familiar para todo el mundo, de la escritura decimal. ¿A qué nos referimos cuando escribimos una expresión como 0,3333...? En realidad, no se trata de una "tira" infinita de 3 sino de una serie, más precisamente:

$$\frac{3}{10}+\frac{3}{100}+\frac{3}{1000}+\frac{3}{10000}+\ldots$$

El resultado no "se parece" sino que es exactamente igual al valor 1/3. De paso, un ejercicio para el lector: ¿cuál es el valor exacto de 0,999....? ¿Será igual a 1, o *casi* igual pero más pequeño?

[7] Existen justamente algunas divergencias en torno a dicha denominación: en algunos textos se dice que dicha serie *converge a infinito*. Aunque existen algunas buenas razones para adoptar esta variante, mantendremos la antes introducida, que es la más frecuente.

La diferencia con la serie anterior puede parecer sutil, pero es decisiva; en este caso, la "suma" no es un número sino que es "infinito". Esto no parece más que una manera de hablar, aunque nuevamente la definición rigurosa de límite es la que permite dar validez a la siguiente escritura:

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\ldots=\infty$$

Uno podría preguntarse, siendo que los términos se acercan cada vez más a 0, cómo es que la serie diverge. Hay muchas maneras de ver esto; una prueba elegante y no tan habitual puede hacerse por el absurdo, de la siguiente forma:

Supongamos que la tesis es falsa; vale decir, que la serie no diverge. En tal caso, como todos los términos son positivos no es difícil ver que debería converger a un valor S. Lo que sigue es más bien informal, aunque puede justificarse debidamente. Si reordenamos los términos colocando primero todos los que tienen denominador impar y luego los que tienen denominador par, nos queda una suma de dos series diferentes, que también convergen a dos valores que llamaremos respectivamente S_I y S_P.

$$S=\left(1+\frac{1}{3}+\frac{1}{5}+\ldots\right)+\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\ldots\right)=S_I+S_P$$

Ahora, si comparamos uno a uno los términos impares con los pares, vemos que $1 > 1/2$, $1/3 > 1/4$, $1/5 > 1/6$, etc. En consecuencia, $S_I > S_P$. Por otro lado, vemos también que

$$S_P=\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\ldots=\frac{1}{2}\left(1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots\right)=\frac{1}{2}S.$$

De esta forma, obtenemos

$$S=S_I+S_P>S_P+S_P=2S_P=S,$$

lo que es absurdo.

En todo caso, vale la pena observar que si bien la serie crece más allá de cualquier valor prefijado, lo hace a un ritmo muy lento. Por ejemplo,

$$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{100}=5{,}1873775176396\ldots$$

$$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{1000}=7{,}48547086055034\ldots$$

$$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{1000000}=14{,}39272672286\ldots$$

Como se ve, al cabo de un millón de términos apenas hemos superado el valor 14; para superar el 100 hacen falta más de 10^{43} = 10000000000000000000000000000000000000000000 términos.[8]

---

[8] Por cierto, el lector no debe imaginar que nos hemos tomado el trabajo de hacer todos estos cálculos, sino que los hemos obtenido con ayuda de una una computadora. Para valores relativamente pequeños de N se puede experimentar por ejemplo con el sencillo programa que aparece en la siguiente página:

http://www.math.utah.edu/~carlson/teaching/calculus/harmonic.html

Sin embargo, a fines de tener una idea más acabada de la velocidad de crecimiento de las sumas parciales, resulta más cómodo emplear la siguiente propiedad, fácil de demostrar, para la suma S_N de los N primeros términos:

Esta impresión de "divergencia lenta" se hace todavía más nítida al observar si en vez del término general $1/n$ ponemos $1/n^s$ para obtener la llamada *serie armónica generalizada*. Si s es un número menor que 1, entonces los términos superan a los de la serie armónica y la serie diverge. En cambio, cuando s es cualquier número mayor que 1 puede probarse que la serie converge; así, el valor $s = 1$ constituye una suerte de *valor crítico.* No importa si s supera a 1 por muy poco; eso basta para que la serie sea ya convergente.[9]

Al cabo de tanto trabajo, estamos en condiciones de dar una excelente noticia: entre una cosa y otra, hemos llegado a la zeta de Riemann, que para cualquier valor $s > 1$ se define precisamente como el valor de la serie armónica generalizada con exponente s que, según dijimos, converge:

$$\zeta(s) = 1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\dots$$

Claro que la historia no acaba aquí, puesto que en realidad debemos ver cómo se extiende la definición de esta función para otros valores de s. Pero vale la pena hacer un breve y fundamental paréntesis para preguntarnos qué tiene que ver todo esto con los números primos. La respuesta a tal pregunta se verá en la próxima sección.

La armonía de los primos

A lo largo de la sección anterior hemos hablado principalmente de la serie denominada *armónica*; no sería de extrañar que a algún lector inquieto le haya surgido una duda más que razonable, incluso una sospecha, respecto de ese nombre. Y la sospecha se torna certidumbre en cuanto comprobamos que el nombre no es casual: la serie armónica tiene que ver con cierta noción de "armonía" que puede remontarse a las especulaciones filosóficas de los pitagóricos y su legendaria *armonía de las esferas*. Sin entrar en detalles, podemos mencionar que su definición proviene de un delicado equilibrio, pues cada término es igual a la llamada *media armónica* entre su antecesor y su sucesor; por otra parte, no debe ya sorprender el hecho de que se encuentra vinculada de forma bastante directa con los *armónicos* en la música.

Lo que sí puede provocar todavía alguna sorpresa es que en tan suave armonía entran a jugar un papel relevante, más bien fundamental, los números primos.

Empecemos por un sencillo ejemplo muy similar al del comienzo de la sección anterior: dado un número p mayor que 1, ¿cuánto vale la suma de la serie cuyo término general es $1/p^n$?

$$\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\frac{1}{p^4}+\dots=?$$

La respuesta es bien precisa y queda como ejercicio para el lector: es una serie convergente, cuya suma es $\frac{1}{p-1}$. Ahora imaginemos que p y q son dos primos distintos, entonces vale:

$$\log N < S_N < 1 + \log N$$

Por ejemplo, el logaritmo de N = 1000000 es 13,815510558..., lo cual permite anticipar, sin necesidad de hacer el cálculo que la suma del primer millón de términos es un valor entre dicho número y 14,815510558... (comparar con el valor "exacto" que vimos anteriormente).

[9] La demostración de este hecho puede verse en cualquier curso básico de análisis matemático, aunque algunos casos particulares se comprueban por métodos aun más elementales. Por ejemplo, para $n = 2$ un argumento "geométrico" se muestra en mi libro *Fragmentos de un discurso matemático (Fondo de Cultura Económica, 2007)*, en donde también se puede ver una notable demostración de la divergencia de la serie armónica propuesta por Johann Bernoulli.

$$\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\frac{1}{p^4}+\dots\right).\left(1+\frac{1}{q}+\frac{1}{q^2}+\frac{1}{q^3}+\frac{1}{q^4}+\dots\right)=\left(1+\frac{1}{p-1}\right).\left(1+\frac{1}{q-1}\right)$$

No sería legítimo hacer uso de la "propiedad distributiva", puesto que los dos factores tienen infinitos términos, aunque la operación que uno haría de manera informal admite en este caso una justificación rigurosa:

$$\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\frac{1}{p^4}+\dots\right).1+\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\frac{1}{p^4}+\dots\right).\frac{1}{q}$$

$$\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\frac{1}{p^4}+\dots\right).\frac{1}{q^2}+\dots=\frac{p}{p-1}.\frac{q}{q-1}$$

En otras palabras,

$$\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\frac{1}{p^4}+\dots\right)+\left(\frac{1}{q}+\frac{1}{pq}+\frac{1}{p^2q}+\frac{1}{p^3q}+\frac{1}{p^4q}+\dots\right)$$

$$+\left(\frac{1}{q^2}+\frac{1}{pq^2}+\frac{1}{p^2q^2}+\frac{1}{p^3q^2}+\frac{1}{p^4q^2}+\dots\right)+\ \dots=\frac{p}{p-1}.\frac{q}{q-1}$$

Ahora prestemos atención a los (infinitos) términos que aparecen en el lado izquierdo de la igualdad: reacomodándolos, vemos que son fracciones de la forma

$$\frac{1}{p^j q^k}$$

en donde j y k toman todos los valores posibles entre los enteros mayores o iguales que 0 (recordemos que $p^0 = q^0 = 1$). Esto permite establecer la igualdad

$$\frac{p}{p-1}.\frac{q}{q-1}=\sum_{n\in A}\frac{1}{n}$$

en donde A es el conjunto formado por todos los números naturales de la forma $p^j.q^k$.

Ahora, ¿qué ocurre si agregamos un nuevo primo r? Repitiendo el procedimiento, resulta

$$\frac{p}{p-1}.\frac{q}{q-1}.\frac{r}{r-1}=\sum_{n\in A}\frac{1}{n}$$

en donde A es ahora el conjunto de los números naturales de la forma $p^j.q^k r^l$, con j, k y l numeros enteros mayores o iguales que 0. Y así sucesivamente, a medida que vamos considerando una cantidad mayor de números primos obtenemos del lado izquierdo un producto con más factores. Al mismo tiempo, del lado derecho queda una suma con más términos, ya que el conjunto A se hace cada vez más grande. Pero: ¿es lícito tomar ahora *todos* los primos? En tal caso, el conjunto A abarcaría la totalidad de los números naturales, pues cada natural mayor que 1 se escribe en forma única como un producto de potencias de factores primos (es el llamado *teorema fundamental de la aritmética*).

El asunto es que los primos son infinitos, de modo que del lado izquierdo de la igualdad tendríamos un dudoso "producto infinito". Sin embargo, eso no debe amedrentarnos: al igual que con las series, los productos infinitos se pueden definir adecuadamente como un límite. Esto requiere ciertas condiciones que escapan a los fines de este trabajo, aunque a grandes rasgos podemos aplicar a tales productos las mismas definiciones de convergencia que para las series. De acuerdo con lo anterior, y empleando ahora el símbolo Π (productoria) para expresar un producto, podríamos aventurar una fabulosa igualdad:

$$\prod_{p \in P} \frac{p}{p-1} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots$$

en donde el conjunto *P* es el de todos los números primos.

Sin embargo, llegado este punto uno debe moderar el entusiasmo y revisar todo con sumo cuidado puesto que, como hemos visto, la serie armónica diverge. ¡Menudo detalle! Eso arruina en buena medida la validez de nuestros argumentos: con las series hay que tomarse las cosas en serio. Aunque dudosa, la "igualdad" anterior permitió a Euler efectuar una notable demostración de la infinitud de los números primos sabiendo que la serie armónica diverge: si la cantidad de primos fuera finita la serie armónica sería igual al producto de un número finito de factores, lo que es absurdo.

Pero vale la pena entender el sentido de esta "demostración", en la que Euler obviamente no buscaba demostrar nada pues ya *sabía* que hay infinitos primos. Sin embargo, su argumento expresa la profunda relación que existe entre la serie armónica y el producto del término izquierdo, que se puede comprobar sin inconvenientes para la serie armónica generalizada: para $s > 1$, vale que

$$\prod_{p \in P} \frac{p^s}{p^s - 1} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots$$

¡Qué gran noticia! El término de la derecha no es otro que la zeta de Riemann: la conexión de su hipótesis con el problema de la distribución de los primos comienza a hacerse más clara. Es hora de extender la función a un campo más amplio, el de los números complejos.

El problema se torna complejo

En la Italia del Renacimiento, matemáticos de la talla de Tartaglia y Cardano se empeñaban en resolver ecuaciones algebraicas que habían escapado al alcance de la matemática antigua: en especial, se ha hecho célebre el método publicado por el segundo de dichos autores en su obra *Ars Magna* para la resolución de la ecuación de tercer grado, una hazaña sorprendente para la época. Claro que la historia está llena de vericuetos y agrias disputas en torno a la paternidad del hallazgo, que finalmente se supo que correspondía a otro matemático llamado Scipione del Ferro. Pero lo que nos interesa aquí es que en su tratado Cardano introduce, con cierto descuido, una verdadera novedad para la época: las raíces cuadradas de números negativos.

Esto es algo totalmente inesperado para aquel que aprendió alguna vez que todo número real elevado al cuadrado da un resultado mayor o igual que cero; las raíces de números negativos, por tanto, deben consistir en objetos por demás extraños, que desafían a las reglas usuales de los números.

Tal es la sensación que se tuvo al comienzo, que motivó que Descartes introdujera para ellos el apelativo de *imaginarios* y que Leibniz llegara a considerar a un número de esa clase como una suerte de *anfibio entre el ser y el no-ser*. Pero, misteriosos o no, las operaciones que se hacían con tales "anfibios" resultaban correctas y se los empezó a usar sin entender quizás a fondo de qué se trataba. Los *números complejos*, que son los que se derivan a partir de introducir las raíces de números negativos, en realidad fueron estudiados en el siglo XVI por Rafael Bombelli pero recién pudieron comprenderse y formalizarse en los siglos posteriores, de la mano de autores como Wallis o Euler y en particular a partir de la representación geométrica que empleamos en la actualidad, presentada a fines del siglo XVIII por un matemático aficionado llamado Argand.

Mirada con nuestros ojos del siglo XXI, la idea es bien simple: se trata apenas de agregar a los números reales un pequeño objeto llamado i (por "imaginario") que funcionará como una raíz cuadrada de -1. Dicho objeto tendrá algunas propiedades curiosas, y por cierto no se puede "adicionar" a una cantidad real, de modo que hará falta agregar muchas cosas más. De hecho, lo que se construye es el conjunto de todas las expresiones formales del tipo $a + bi$, en donde tanto a como b son números reales; a continuación, no es complicado definir allí operaciones de suma y producto de tales expresiones de modo que se respeten las propiedades que esperamos de ellas:

SUMA: $(a + bi) + (c + di) = (a + c) + (b + d)i$

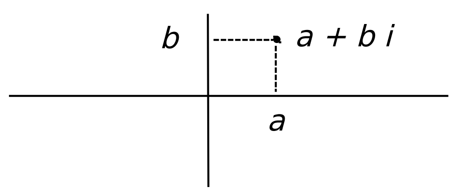
PRODUCTO: $(a + bi).(c + di) = (ac - bd) + (ad + bc)i$

De estas dos definiciones, sin duda la menos obvia es la segunda. Sin embargo, pronto se hace "evidente", en tanto uno pretende que para estos "números" complejos valgan, como dijimos, las propiedades habituales de la suma y el producto de reales. Vista de esta manera, la definición del producto es la única posible, ya que

$$(a + bi).(c + di) = ac + bic + adi + bidi = ac + bdi^2 + (ad + bc)i,$$

y se obtiene el resultando apelando ahora al hecho de que $i^2 = -1$.

La representación de Argand, que terminó de quitar a estos números su misterio, consiste en pensar a las cantidades a y b (llamadas respectivamente *parte real* y *parte imaginaria* del número) como las dos coordenadas del plano cartesiano.



A esta altura, tenemos ya casi todos los elementos necesarios para esbozar el significado pleno de la hipótesis de Riemann, aunque para eso falta un último paso: extender la función ζ al plano de los números complejos. El lector que haya llegado hasta aquí puede verse tentado de tomar un breve descanso y aceptar, sin más preámbulos, el hecho de que dicha extensión es posible. En tal caso, el consejo más conveniente es que saltee la próxima sección y pase directo al final del artículo. Aunque si ha llegado hasta aquí, eso demuestra que tiene agallas suficientes como para hacer frente a un último desafío antes de ver los detalles finales de la construcción.

Zeta de *z*

Los números complejos, tal como los presentamos en la sección previa, suelen escribirse en forma genérica por medio de la variable z. Esto es apenas una costumbre, al igual que el uso de la x para referirnos a una variable real, pero justifica el título de esta nueva sección: de lo que se trata es de encontrar una expresión válida para $\zeta(z)$, pero considerando que z ya no es como antes un número real mayor que 1 sino un número complejo. Para ser más precisos, la función estará definida en todo el plano complejo salvo en el valor $z = 1$, en donde tendrá lo que se denomina una *singularidad*. Esto es sin duda razonable, pues en nuestra definición previa es fácil ver que si s se aproxima a 1 el valor de $\zeta(s)$ se hace cada vez más grande.

Para empezar, procuraremos entender el significado de $\zeta(z)$ para $z = a + bi$ con $a > 1$. La pregunta básica es: ¿existe alguna interpretación razonable de la expresión

$$\zeta(z) = 1+\frac{1}{2^z}+\frac{1}{3^z}+\frac{1}{4^z}+\dots$$

cuando z es un número complejo? Para ello, deberíamos en principio dar algún sentido a los denominadores de la forma n^z: ¿qué significa elevar un número a un exponente complejo?

La respuesta, quizás sorprendente, es que en general esto no se puede establecer en forma única, ni para todos los números a la vez; sin embargo, en nuestro caso específico hay una forma razonable de pensarlo. En principio, recordemos la magnífica fórmula establecida por Euler, que revela una íntima relación entre la función exponencial y las funciones trigonométricas:

$$e^{ix} = cos(x) + i\ sen(x).$$

Para quien no conozca las razones profundas de esta igualdad, todo el asunto no parecerá más que una misteriosa manera de escribir; como sea, nos permite ver que al menos en ciertos casos es posible pensar en un exponente que no sea real. Más en general, dado cualquier $z = a + bi$, se puede definir la exponencial e^z de modo "evidente":

$$e^z = e^{a+bi} = e^a e^{bi} = e^a\ (cos(b) + i\ sen(b))$$

Pero esto puede extenderse para muchos casos en donde la base no es e: por ejemplo, a partir del hecho de que un número real positivo u puede escribirse como

$$u = e^{log(u)}$$

resulta de lo más legítimo definir u^z de la siguiente forma:

$$u^z = e^{log(u)z}$$

El artilugio puede parecer tramposo, pero resulta de gran utilidad para el caso que estamos considerando, en el que solo necesitamos tener definido el valor de n^z para n natural y $z = a + bi$:

$$n^z = e^{log(n)z} = n^a e^{log(n)bi}$$

Quizá esto siga resultando en buena medida oscuro, aunque es posible justificarlo con todo cuidado.[10] Y, por fin, si $a > 1$ es fácil ver que la fórmula anterior para $\zeta(z)$ -que ahora es una serie de números complejos- converge.

La extensión de ζ para los restantes valores del plano (exceptuando, como dijimos, $z = 1$) fue obtenida por Riemann mediante una técnica muy importante del análisis complejo, que se conoce como *continuación analítica*. Lo que resulta es una función difícil de imaginar en forma directa, aunque se puede probar que satisface la siguiente relación:

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

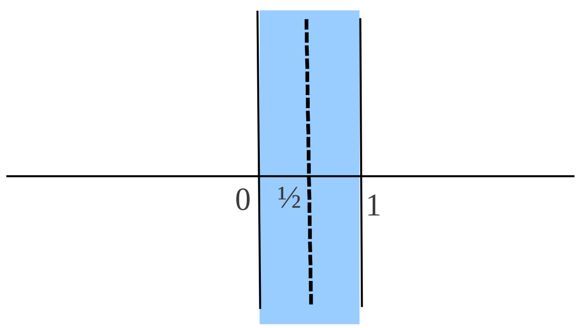
En esta fórmula aparecen dos nuevos elementos inquietantes: por un lado, la función Γ, de múltiples aplicaciones y muy conocida en la teoría de probabilidades; por otro, la antigua y entrañable función seno, pero extendida a los números complejos. Esto puede sonar raro, pero permite ya ver cuáles son los ceros "triviales" de la función ζ, pues sabemos que $\text{sen}(k\pi) = 0$ para todo k entero:

[10] Debemos señalar que los "cuidados" a los que hacemos referencia no son excesivos, sino que obedecen al hecho de que en el terreno de los números complejos muchas cosas no son como uno podría esperar. Por ejemplo, teniendo en cuenta la anterior fórmula de Euler vale $e^{2\pi i} = 1$, y si x es un número real uno diría entonces que $(e^{2\pi i})^x = 1^x = 1$. Sin embargo, También podríamos argumentar que $(e^{2\pi i})^x = \cos(2\pi x) + i\ \text{sen}(2\pi x)$, lo cual no es 1 sino que para los diferentes valores de x recorre toda la circunferencia de radio 1. Vale la pena preguntarse: ¿cuál es la falla?

cuando z es un entero par menor que 0, la zeta debe anularse. En cambio, si se trata de un entero par pero mayor que 0, la cosa cambia pues en tal caso $\Gamma(1 - z)$ se hace infinito y en cierta medida se "compensa" con el cero de $sen(\pi z/2)$. Algo similar ocurre para z=0, aunque en este caso el cero de $sen(\pi z/2)$ se ve compensado por la propia ζ, ya que $\zeta(1\text{-}0) = \infty$. Los detalles quedarán para el lector interesado en profundizar en estas delicadas cuestiones.[11]

En definitiva: ¿ha probado alguien la hipótesis de Riemann?

Como el lector podrá recordar, entre las numerosas anécdotas que circulan en relación a la famosa conjetura hemos mencionado la de Hilbert y su eventual resurrección, a la que remite el título de esta última sección. A grandes rasgos, la analogía parece bastante oportuna, ya que tras unas cuantas páginas preparatorias (y algo arduas) podemos sentir que "volvemos a la vida" con renovadas energías. ¿Qué dice la hipótesis? Que, además de los ceros "triviales" que mencionamos al fin de la sección previa, la función ζ no se anula en ningún valor $z = a + bi$ con a distinto de 1/2. Se han encontrado muchos, infinitos ceros no triviales de la función y -hasta el momento- todos ellos tienen parte real 1/2. Pero no se ha *demostrado* que esto tenga que ser así para cualquier nuevo cero que aparezca. Desde el punto de vista geométrico, lo que esto significa es que los ceros no triviales de ζ deben caer todos sobre la línea punteada:



Cabe decir que la incertidumbre no es absoluta: desde 1859 a la fecha se han probado muchas cosas sobre los ceros no triviales de la función de Riemann. Por ejemplo, se ha probado que todos caen dentro de la franja sombreada, que es la de aquellos números con parte real entre 0 y 1: este resultado bastó para probar el mencionado teorema de los números primos. Pero la conjetura, en su forma original, permanece sin respuesta. Se anunciaron hasta la fecha muchas demostraciones diferentes, tanto de la conjetura como de su negación, y en todas se ha encontrado algún error. A su vez, existen todavía algunas demostraciones que no han llegado a revisarse por completo: quién sabe, tal vez alguna de ellas sea por fin correcta. Pero el panorama no es nada claro: la revisión solo puede ser llevada a cabo por los verdaderos expertos en el tema, quienes deben dedicar mucho tiempo a leer línea por línea extensas páginas. El lector interesado en conocer algunas de las demostraciones fallidas, así como algunas de las pruebas todavía no chequeadas tanto del teorema como de su negación, puede consultar en:

http://empslocal.ex.ac.uk/people/staff/mrwatkin//zeta/RHproofs.htm

En lo que respecta a este artículo, podemos darnos por satisfechos por el momento y aguardar con paciencia a ver si la hipótesis figura en la lista de problemas no resueltos que la comunidad

[11] El lector podría observar que el factor $\Gamma(1 - z)$ también se hace infinito cuando z es un impar positivo; sin embargo, si z es además mayor que 1 entonces $\zeta(1 - z)$ es 0, y otra vez se produce una especie de "compensación" del tipo "0.∞".

matemática publique en los albores del próximo siglo. Tras una historia de un siglo y medio, la espera no parece tan larga: al fin y al cabo, solo restan unos noventa años.