La Naturaleza Trans-Pitagórica de los Números Primos

Miguel Ángel Rodríguez-Roselló (*)

Resumen

En este artículo se estudian los números primos y compuestos desde el punto de vista de los dos modos de conciencia: 1) la conciencia profunda, intuitiva y sintética; 2) la conciencia superficial, racional y analítica. Esta dualidad universal se manifiesta, respectivamente, en los números primos y compuestos.

Según el principio de causalidad descendente, lo superficial es siempre una manifestación de lo profundo, y es imposible expresar lo profundo desde lo superficial. Por lo tanto, los números compuestos son manifestaciones de los números primos, y los números primos son inexpresables. Esta inexpresabilidad de los primos se manifiesta, se justifica y se fundamenta en la suma y resta de cuadrados, es decir, en las expresiones pitagóricas duales a^2+b^2 y a^2-b^2:

- Los números primos impares –que son todos los primos excepto el 2– se dividen en dos clases: los de tipo $4k+1$ y los de tipo $4k-1$. Según el teorema de Navidad de Fermat, todos los primos de tipo $4k+1$ se pueden expresar de manera única como suma de cuadrados. Los números primos de tipo $4k-1$ son inexpresables desde el punto de vista pitagórico, es decir, son inexpresables como suma o resta de cuadrados, excepto de manera trivial como diferencia entre los cuadrados de dos números consecutivos (como todos los números impares).

- Hay muchas razones para considerar que los primos tipo $4k+1$ no son verdaderos primos, entre ellas –principalmente– porque no son primos gaussianos. Desde este punto de vista, la inexpresabilidad de los números primos –su naturaleza trans-pitagórica– concuerda con la idea de que desde lo superficial (los números compuestos) no puede expresarse lo profundo (los números primos).

En definitiva, no hay nada extraño ni misterioso ni complejo en el tema de los números primos. Al contrario, es algo fundamentalmente simple por su estrecha relación con el teorema de Pitágoras. La clave de la comprensión de los números primos reside en la suma/resta de cuadrados, es decir, las formas duales del teorema de Pitágoras. El teorema de Pitágoras es el teorema más fundamental de la matemática. El teorema de Pitágoras es un teorema de la conciencia, el Santo Grial de la matemática.

Adicionalmente, este estudio ha conducido al descubrimiento de que existen 7 tipos de números impares desde el punto de vista de las expresiones pitagóricas: 2 en la rama $4k-1$ y 5 en la rama $4k+1$. El tipo inexpresable de la rama $4k-1$ corresponde a la clase de los "verdaderos" números primos.

Conceptos Básicos Previos

Los números primos

Los números primos son los números naturales que solo son divisibles por sí mismos y por la unidad. Los primeros números primos son:

(*) Doctor en Informática, Licenciado en Física, Master en Ingeniería del Conocimiento.
Email: marosello@telefonica.net

2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, ….

El teorema fundamental de la aritmética afirma que todo número natural mayor que 1 es primo o puede expresarse como un producto único de dos o más primos (iguales o distintos). Este teorema da lugar a lo que podemos denominar "el problema fundamental de la aritmética": dado un número natural $n>1$, encontrar sus factores primos.

Los números que no son primos se denominan "compuestos", es decir, son el producto de dos o más primos. Por lo tanto, todo número es o primo o compuesto. Un número compuesto establece una relación (producto) entre números primos. Por ejemplo, $72 = 2^3 \times 3^2$.

Un conjunto de números naturales se dice que son coprimos, primos relativos o primos entre sí, si no tienen ningún factor común, es decir que su m.c.d. es 1. Por ejemplo, 5, 12 y 17 son coprimos.

Los números primos constituyen las claves de los modernos sistemas de encriptado que se utilizan para seguridad en las comunicaciones. Se utilizan números grandes que hay que descomponer en factores primos. Esta tarea requiere muchos recursos computacionales y temporales. Por ejemplo, lo utiliza el sistema asimétrico RSA de clave pública para transmisión de datos de forma segura. La clave pública se basa en el producto de dos números primos grandes. Cualquiera puede usar la clave pública para encriptar un mensaje. Si el destinatario conoce los primos componentes, entonces puede descifrar fácilmente el mensaje.

Los números primos se consideran "la corona" de la teoría de números. Esta teoría, que trata de las propiedades de los números naturales y sus relaciones, es el área más pura y la más antigua de las matemáticas. Puede parecer algo elemental, pero en realidad la teoría de números es una de las áreas más profundas y difíciles de la matemática. También se la denomina "alta aritmética", una aritmética que aborda problemas complejos como el último teorema de Fermat, la hipótesis de Riemann, la conjetura de los infinitos primos gemelos, la conjetura de Goldbach, etc. "La matemática es la reina de las ciencias y la teoría de números es la reina de las matemáticas" (Gauss) [1].

La teoría de números tiene dos ramas: la aditiva y la multiplicativa. Paradójicamente, la rama multiplicativa –que es más compleja que la aditiva– es la que más se ha desarrollado, y tiene una antigüedad que se remonta a Pitágoras. La rama aditiva es mucho más joven. Se empezó a desarrollar con Euler, y trata de cómo un número natural puede expresarse como suma de otros números naturales.

La teoría de números –a pesar a su nombre– tiene también una parte experimental. Teoría y práctica se complementan. Normalmente, la parte experimental viene primero y conduce a cuestiones que luego hay que tratar de responder a nivel teórico. Hoy día, la parte experimental suele estar apoyada por aplicaciones informáticas.

Propiedades de los números primos

Los números primos tienen muchas propiedades. Aquí nos interesa destacar las siguientes:

- Desde Euclides se sabe que el número de números primos es infinito, como el de los números naturales.

- Tradicionalmente, el 1 no se considera primo, aunque cumple el criterio de primalidad. El 1 no es compuesto porque no puede descomponerse en primos más pequeños, a menos que incluyamos los enteros negativos, en cuyo caso, el 1 sería compuesto porque $1 = (-1)\times(-1)$. A su vez, el −1 no sería primo si se consideraran números complejos, pues $-1 = i\times i$, siendo i la unidad imaginaria. El 1 es el elemento neutro de la multiplicación y está implícito en todos los números (primos y compuestos). Aunque el 1 se considera el primer número natural, realmente representa el absoluto, la unidad previa a la creación de la dualidad. Así que el 2 se considera el primer número primo.

- Excepto el 2 –que es el único primo par y el primo más pequeño–, todos los demás números primos son impares.

- Los divisores 1 y el propio número n se consideran "triviales". Los otros divisores se denominan "propios". Por lo tanto todo divisor propio d de n cumple $1 < d < n$.

- Con excepción del 3, la suma de los dígitos de un número primo no puede ser múltiplo de 3.

- Los números primos –con la excepción del 2 y el 5– acaban en 1, 3, 7 o 9. Los números que acaban en 5 no son primos porque son múltiplos de 5. En este sentido, podemos decir que solo hay 4 tipos o clases de números primos.

- Los números primos se van separando progresivamente. El denominado "Teorema de los Números Primos" establece que el número de primos entre 1 y n se aproxima a $\pi(n) = n/\ln(n)$ cuando n tiende a infinito, siendo $\ln(n)$ el logaritmo natural de n.

  La separación entre dos números primos consecutivos es tan grande como se quiera. En efecto, entre $n!+2$ y $n!+n$ no existe ningún primo, pues $n!+2, n!+3, \ldots, n!+n$ son divisibles respectivamente por $2, 3, \ldots, n$. Por ejemplo, si $n = 5$, $n! = 120$, y tenemos la secuencia $120+2, 120+3, 120+4, 120+5 = 122, 123, 124, 125$, que son todos números compuestos. Eligiendo n suficientemente grande, tenemos $n-1$ números compuestos consecutivos.

Tipos de números primos

Hay muchos tipos de números primos. Aquí solo nos interesan los siguientes:

- Los primos gemelos son primos consecutivos que difieren en 2. Los primeros primos gemelos son:

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), ...

El 5 es el único número primo que pertenece a dos primos gemelos.

Se conjetura que hay infinitos primos gemelos. La mayoría de los matemáticos creen que es cierta, pero aún no se ha demostrado.

- Un número gaussiano es un número complejo de la forma $a+bi$, siendo a y b números enteros (uno de ellos puede ser cero) e i la unidad imaginaria. Un número primo gaussiano es un número gaussiano que no se puede factorizar en otros números gaussianos.

  Algunos números primos no son primos gaussianos porque se pueden factorizar en el plano complejo. Por ejemplo, el número primo 17 no es primo gaussiano porque se puede factorizar como $(4+i)(4-i) = 4^2+1 = 17$. En general, un número natural que se pueda expresar como suma de dos cuadrados (a^2+b^2) no es primo gausiano pues se puede factorizar de la forma $(a+bi)(a+bi)$.

  Ejemplos de primos gaussianos son: $1+i$, $1-i$, $10+9i$, $14+i$, $17+2i$. En general, si $a+bi$ es primo gaussiano, también lo es su conjugado $(a-bi)$.

  Los números naturales que son primos gaussianos son: 3, 7, 11, 19, 23 …, que son todos de la forma $4k-1$ ($k = 1, 2, \ldots$).

- Los primos pitagóricos –descubiertos por Diofanto de Alejandría– son los que pueden expresarse como suma de dos cuadrados: $p = a^2 + b^2$. Por ejemplo:

  $5 = 1^2 + 2^2$ $13 = 2^2 + 3^2$ $17 = 1^2 + 4^2$ $29 = 2^2 + 5^2$ $37 = 1^2 + 6^2$

  Se sabe que el número de primos pitagóricos y no pitagóricos hasta un número n es aproximadamente igual.

  Hay números que pueden expresarse como suma de cuadrados pero que no son primos. Por ejemplo,

  $25 = 3^2 + 4^2$ $45 = 3^2 + 6^2$ $65 = 1^2 + 8^2$

  Los primeros primos pitagóricos son:

  2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, …

  El 2 corresponde a la expresión $1^2+1^2 = 2$, que es único primo pitagórico par. Fermat descubrió que los primos pitagóricos impares p tienen la propiedad de ser de la forma $4k+1$, es decir, son congruentes entre sí y con 1 módulo 4: $p \equiv 1 \pmod 4$.

Ternas Pitagóricas

Una terna pitagórica es un conjunto ordenado de tres números naturales (x, y, z) que corresponden a los lados de un triángulo rectángulo, en donde x e y son los catetos y z es la hipotenusa. Es decir, se cumple el teorema de Pitágoras: $x^2+y^2 = z^2$. Un triángulo rectángulo cuyos lados forman una terna pitagórica se denomina "triángulo pitagórico".

Excluyendo la terna trivial (1, 1, 2), las ternas pitagóricas tienen las propiedades siguientes:

- Como x e y tienen distinta paridad, z debe ser impar. Como x e y son intercambiables, podemos suponer que x es impar. Por lo tanto, una terna pitagórica es de tipo simétrico: (impar, par, impar).

- Las ternas pitagóricas tienen la forma $(a^2–b^2, 2ab, a^2+b^2)$, con a>b, pues se cumple que $(a^2–b^2)^2 + (2ab)^2 = (a^2+b^2)^2$. Puesto que $a^2–b^2$ y a^2+b^2 son impares, a y b tienen distinta paridad. Dada la terna pitagórica (x, y, z), los valores de a y b correspondientes son:

  $$a = \sqrt{((z+x)/2)} \qquad b = \sqrt{((z–x)/2)}$$

- Vamos a denominar "expresión pitagórica positiva" a toda expresión del tipo a^2+b^2, siendo a y b números naturales de distinta paridad. A nivel geométrico, el número correspondiente ($n = a^2+b^2$) tiene la propiedad de que su raíz cuadrada ($\sqrt{n}$) es la hipotenusa de un triángulo rectángulo de catetos a y b. Los números de este tipo pueden ser primos o no, pero no son primos gaussianos porque se pueden descomponer en factores: $a^2+b^2 = (a + bi)(a – bi)$.

- Vamos a denominar "expresión pitagórica negativa" a toda expresión del tipo $a^2–b^2$, siendo a y b números naturales de distinta paridad y $a>b$. Llamando n al número correspondiente ($n = a^2–b^2$), entonces a nivel geométrico, a es la hipotenusa de un triángulo rectángulo de catetos $\sqrt{n}$ y b. Por ejemplo:

  $$15 = 4^2–1^2, \;\; 33 = 7^2–4^2, \;\; 91 = 10^2–3^2$$

- Las ternas pitagóricas conectan las expresiones pitagóricas positivas y negativas. Es decir, toda terna pitagórica posee dualidad a nivel de signo entre los términos extremos ($a^2–b^2$ y a^2+b^2). Por ejemplo, $(4^2–1^2, 8, 4^2+1^2) = (15, 8, 17)$.

- Existe una relación entre los números gaussianos y las ternas pitagóricas. Un número gaussiano, que es un número complejo $c = a+bi$, con a y b enteros, tiene como norma $|c| = \sqrt{(a^2+b^2)}$. Si multiplicamos c por sí mismo, tenemos $c^2 = a^2–b^2+2abi$, en donde la parte real y la parte imaginaria son los dos primeros términos de de una terna pitagórica (los dos catetos) y su norma al cuadrado es el tercer término (la hipotenusa): $|c^2| = a^2+b^2$.

- Hay dos tipos de ternas pitagóricas: primitivas y derivadas. Las ternas primitivas (x, y, z) son las que cumplen m.c.d.(x, y, z) = 1, es decir, que no tienen ningún factor común (son coprimos). Las primeras ternas pitagóricas primitivas con x<100 son:

  (3, 4, 5), (5, 12, 13), (7, 24, 25), (8, 15, 17), (9, 40, 41), (11, 60, 61), (12, 35, 37),

(13, 84, 85), (16, 63, 65), (20, 21, 29), (28, 45, 53), (33, 56, 65), (36, 37, 85), (39, 80, 89), (48, 55, 73), (65, 72, 97)

Hay infinitas ternas pitagóricas primitivas. Euclides lo demostró de la manera siguiente. Todo número impar se puede expresar como diferencia entre los cuadrados de dos números consecutivos. La fórmula es: $n = a^2–b^2$, siendo $a = (n+1)/2$ y $b = (n–1)/2$. A partir de esta fórmula, se construye la terna $(a^2–b^2, 2ab, a^2+b^2)$. Por ejemplo, para n=7, tenemos a=4 y b=3, y la terna es $(4^2–3^2, 24, 4^2+3^2) = (7, 24, 25)$. Como hay infinitos números impares, hay infinitas ternas pitagóricas primitivas.

Las ternas derivadas de una terna primitiva (x, y, z) son múltiplos de tipo (nx, ny, nz), con n>1. Hay, por lo tanto, infinitas ternas pitagóricas derivadas de una terna pitagórica primitiva. Por ejemplo, para la terna pitagórica (3, 4, 5), sus derivadas son: (6, 8, 10), (9, 12, 15), (12, 16, 20), etc.

- La terna pitagórica más pequeña es (3, 4, 5), que corresponde al llamado "triángulo egipcio", en donde 3 y 5 son los dos primeros números primos impares.

- Todo número natural a forma parte de una expresión pitagórica positiva a^2+b^2, y esta a su vez forma parte de una terna pitagórica. Por ejemplo, $1^2+2^2 = 5$, $2^2+3^2 = 13$, $3^2+4^2 = 25$, etc.

- En una terna pitagórica $(a^2–b^2, 2ab, a^2–b^2)$, $a^2–b^2$ puede ser primo o compuesto, $2ab$ es compuesto (es par) y a^2+b^2 puede ser primo o compuesto. Ejemplos:

  $(3, 4, 5) = (2^2–1^2, 4, 2^2+1^2)$ (3 y 4 son primos)
  $(15, 8, 17) = (4^2–1^2, 8, 4^2+1^2)$ (15 es compuesto, 17 es primo)
  $(23, 264, 265) = (12^2–11^2, 264, 11^2+12^2)$ (23 es primo, 265 es compuesto)
  $(63, 16, 65) = (8^2–1^2, 16, 8^2+1^2)$ (63 y 65 son compuestos)

- La llamada "hipótesis H" de Schinzel-Sierpinski [Ribenboim, 1996] afirma que hay infinitas ternas pitagóricas que contienen dos primos (los elementos primero y tercero, puesto que el segundo es par).

  Una terna pitagórica prima es una terna cuyos elementos extremos son primos. Es una terna primitiva. El triángulo rectángulo correspondiente se denomina "triángulo pitagórico primo". Las 10 primeras ternas pitagóricas primas son:

  $(3, 4, 5) = (2^2–1^2, 4, 2^2+1^2)$
  $(5, 12, 13) = (3^2–2^2, 12, 3^2+2^2)$
  $(11, 60, 61) = (6^2–5^2, 60, 6^2+5^2)$
  $(19, 180, 181) = (10^2–9^2, 180, 10^2+9^2)$
  $(29, 420, 421) = (15^2–14^2, 420, 15^2+14^2)$
  $(59, 1740, 1741) = (30^2–29^2, 1740, 30^2+29^2)$
  $(61, 1860, 1861) = (31^2–30^2, 1860, 31^2+30^2)$
  $(71, 2520, 2521) = (36^2–35^2, 2520, 36^2+35^2)$
  $(79, 3120, 3121) = (40^2–39^2, 3120, 40^2+39^2)$

$$(101, 5100, 5101) = (51^2–50^2, 5100, 51^2+50^2)$$

Hay solo una terna pitagórica prima que contiene dos primos gemelos (p y p+2): la terna primitiva arquetípica (3, 4, 5).

Se conjetura, como en el caso de los primos gemelos, que hay infinitas ternas pitagóricas primas.

- Existen ternas pitagóricas que comparten un mismo cateto. Por ejemplo, (15, 112, 113), (15, 20, 25), (15, 36, 39), (15, 8, 17). En cambio, no existen ternas pitagóricas que compartan el tercer término (la hipotenusa), pues toda expresión pitagórica de tipo $x^2+y^2 = z^2$ es única.

La Cuestión del Patrón de los Números Primos

La situación actual

La estructura del conjunto de los números primos es aparentemente irregular, sin ningún orden ni patrón cuantitativo específico, pero con un patrón cualitativo de tipo general: los números primos se van distanciando progresivamente entre sí. Los números primos son independientes entre sí, sin relaciones multiplicativas a nivel de los números naturales. Solo tienen relaciones aditivas particulares, pero sin patrón general conocido.

Todos los intentos de obtener el patrón de los números primos han fracasado. Se suele decir que los números primos es lo que queda cuando se eliminan todos los patrones de los números naturales. Se han encontrado patrones parciales y particulares, pero hasta ahora no se ha encontrado un patrón de tipo general. No obstante, se sigue buscando por dos razones: 1) porque se cree que algo tan fundamental como los números primos debe tener un patrón; 2) porque la matemática es una disciplina lógica, por lo que la distribución de los números primos en la recta real debe estar sujeta a las reglas de la lógica y ser totalmente determinista.

La búsqueda de ese patrón ha fascinado a matemáticos profesionales y aficionados a lo largo de la historia, hasta ahora sin resultado. Algunos autores creen que este tema podía ser indecidible (en el sentido de Gödel). Algunas opiniones pesimistas al respecto son:

- “Los matemáticos han tratado en vano hasta hoy descubrir algún orden en la secuencia de los números primos, y tenemos razón para creer que es un misterio en el que la mente humana no penetrará nunca” (Leonhard Euler) [2].
- “Dios no juega a los dados con el universo, pero algo extraño pasa con los númerosprimos” (atribuido a Paul Erdös) [3].
- “Pasarán otro millón de años antes de que entendamos los números primos” (Paul Erdös) [4].
- “Los números primos son el mayor misterio de la matemática” (Marcus du Sautoy) [5].

Se cree que, si se descubriera el patrón de los primos:

- Sería el "Santo Grial" matemático. Podría arrojar luz sobre la naturaleza última y profunda de los números naturales, de la matemática e incluso del universo. En definitiva, quizás sea la clave de la Teoría de Todo.

  Entender los números primos es entender todos los mundos posibles porque los números primos trascienden la realidad física. Los números primos son reales e indestructibles y están en todos los mundos posibles.

- Tendría efectos sobre diversos campos específicos, especialmente los de tipo profundo, como la genética y la física cuántica.

  Según Igor V. Volovich [6], las entidades fundamentales del universo no son las partículas físicas (electrones, quarks, etc.) ni los campos cuánticos, ni las cuerdas, sino los números naturales, las entidades matemáticas fundamentales. Y como los números naturales se construyen a partir de los números primos, las entidades fundamentales del universo son los números primos. Esto lo justifica porque a nivel físico profundo, a distancias inferiores a la longitud de Planck (la distancia más pequeña capaz de ser medida) no rigen los conceptos habituales (macroscópicos) de espacio 3D, ni tiempo lineal ni la geometría euclidiana convencional.

  Galileo afirmaba que el universo está escrito en el lenguaje de las matemáticas. Pero Max Tegmark [7] va más allá: el universo es una estructura matemática; la naturaleza más profunda de la realidad es de tipo matemático; la matemática es el único universo que existe.

- Supondría una experiencia de conciencia trascendente y unificada de la realidad interna y externa. Según Chaitin [8], "comprender es comprimir", es decir, toda forma de conocimiento y comprensión se basa necesariamente en la compresión. En el caso de encontrar el patrón de los números primos, lo infinito se comprimiría en lo finito.

- Se simplificarían las demostraciones de los teoremas matemáticos de la teoría de números (como el último teorema de Fermat), y podrían resolverse problemas matemáticos pendientes como la hipótesis de Riemann, la conjetura de Goldbach, la conjetura de los infinitos primos gemelos, etc. A nivel profundo todo se simplifica porque desde ese nivel es posible contemplar con claridad todo lo manifestado.

- Se debilitarían los sistemas criptográficos de clave pública de seguridad en las comunicaciones basados en la factorización de grandes números primos.

Los patrones envolventes de los números primos

Aunque no se ha encontrado el patrón de los números primos, se intenta acotar ese patrón mediante diferentes patrones envolventes, es decir, patrones que engloben a todos los números primos. Los más importantes son:

- El patrón $2k+1$.
  Con excepción del 2, todos los números primos son impares. Por lo tanto, el patrón n

= $2k+1$, con $k = 1, 2, 3, 4,\ldots$ es el patrón envolvente de todos los números primos impares. Expresado de otro modo, $n \equiv 1$ (módulo 2). De esta forma se criban la mitad (50 %) de los números naturales. Los números primos impares están siempre al lado de un número compuesto. Basta con hacer $p-1$ o $p+1$ para encontrar un número par (que es un número compuesto). Un primo $p = 2k+1$ está siempre "escoltado" por los números pares $2k$ y $2k+2$.

- El patrón $4k\pm1$.
  Los números impares se pueden dividir en dos ramas:

  1. $n_1 = 4k-1$ ($k = 1, 2, 3, \ldots$): 3, 7, 11, 15, 19,… Es decir, $n_1 \equiv -1$ (módulo 4).
  2. $n_2 = 4k+1$ ($k = 1, 2, 3, \ldots$): 5, 9, 13, 17, 21,… Es decir, $n_2 \equiv 1$ (módulo 4).

  La diferencia entre los números de ambas ramas para el mismo k es $(4k+1) - (4k-1) = 2$.

- El patrón $6k\pm1$.
  Con excepción del 2 y el 3, todos los números primos caen dentro del patrón $6k\pm1$. Este patrón resulta de considerar 6 expresiones:

  $$6k-3,\ 6k-2,\ 6k-1,\ 6k,\ 6k+1,\ 6k+2$$

  y descartar las que son múltiplos de 2 o de 3. De esta forma se criban 4/6 = 2/3 (66,666… %) de los números naturales.

- Otro posible patrón se basa en considerar el producto de los tres primeros números primos: $2\times3\times5 = 30$. En este caso, hay 30 expresiones, en las que habría que descartar las expresiones que son múltiplos de 2, 3 o 5, quedando finalmente $30k\pm1$, $30k\pm7$, $30k\pm11$, $30k\pm13$. De esta forma se criba el $(30-8)/30 = 22/30$ (73,333… %) de los números naturales.

  También se pueden elegir más números primos iniciales. Con este sistema se van cribando sucesivamente los múltiplos de 2 y 3; de 2, 3 y 5; de 2, 3, 5 y 7; etc. Son fórmulas parciales que en conjunto producen envolventes de los números primos. Cuanto mayor es el número de factores primos iniciales, mayor acercamiento al patrón de los números primos, pero más compleja es la fórmula. Un ajuste final mediante este sistema es imposible porque implica el infinito. En este sentido hay una analogía con los números irracionales. Con este sistema se da la paradoja de que la fórmula que expresa la base de los números primos se basa en los propios números primos.

Los aspectos a considerar

En el tema de la búsqueda del posible patrón de los números primos hay que tener en cuenta varios aspectos o factores:

- La cuestión del producto.
  Se suele afirmar que los números primos son los "bloques constructivos" de los

números naturales, de la misma forma que los átomos son los bloques constructivos de la materia y las células los bloques constructivos de los seres vivientes. Esto no es cierto, porque en estos casos los bloques constructivos se basan en la suma, no en el producto.

También se suele establecer una analogía entre una expresión compuesta, como $2^2 \times 3 \times 5^3$, y una fórmula química como por ejemplo $C_6H_{12}O_6$ (la fórmula de la glucosa), diciendo que los números primos son como átomos. Esto tampoco es cierto. En primer lugar, porque el número de átomos es finito y el número de primos es infinito. En segundo lugar, porque la relación química es aditiva, no multiplicativa. En tercer lugar, porque hay fórmulas que corresponden a una estructura cíclica como el benceno (C_6H_6). Solo hay una analogía superficial, de mera forma.

La dificultad en encontrar el patrón de los números primos se debe a que todo se basa en el producto de números naturales. De hecho, deberíamos decir que "los primos son los bloques constructivos multiplicativos de los números naturales". Es imposible establecer una relación multiplicativa entre los números primos que no involucre a los números racionales. El camino correcto para encontrar ese posible patrón debe basarse en la rama aditiva de la teoría de números: la suma, que es una operación más sencilla y fundamental que el producto. Desde el punto de vista de la suma, solo hay un número que podemos calificar de "primo" o "primario", que es el 1. Todos los demás son números compuestos.

Una forma de establecer relaciones con la suma es considerar el tema de las particiones de un número natural. Dado un número natural *n*, hay un número de particiones posibles de dicho número. Así como la descomposición de un número en productos de números primos es única, la descomposición de un número en sumas no es única. Llamando $P(n)$ al número de particiones de *n*, tenemos por ejemplo:

$P(2) = 2$ (2, 1+1)
$P(3) = 3$ (3, 2+1, 1+1+1)
$P(4) = 5$ (4, 3+1, 2+2, 2+1+1, 1+1+1+1)
$P(5) = 7$
$P(10) = 42$
$P(100) = 190.569.292$

Estudiados por Ramanujan, Ken Ono y su equipo dieron con la primera fórmula para calcular directamente $P(n)$ a partir de n. Descubrieron que estos números tienen estructura fractal [Bruiner & Ono, 2011].

- Los modos de conciencia.
  Como es sabido, existen dos modos de conciencia:

  1. La conciencia intuitiva, profunda, conceptual, sintética, creativa, general, global, imaginativa, cualitativa, paralela, continua, etc. Se suele asociar al hemisferio derecho del cerebro. La denominaremos, para simplificar, "conciencia HD".

2. La conciencia racional, superficial, formal, analítica, particular, cuantitativa, secuencial, discreta, etc. Se suele asociar con el hemisferio izquierdo del cerebro. La denominaremos, para simplificar, "conciencia HI".

La conciencia completa surge cuando ambos modos de conciencia están conectados. Esta conexión es tal que lo particular es una manifestación de lo general. En este sentido, la conciencia HD es superior a la conciencia HI. Lo particular nunca puede estar aislado. Debe estar siempre ligado a algo general o universal. Esta conexión es precisamente la semántica de lo particular, lo que le confiere significado.

Esta dualidad universal se manifiesta en la dualidad particular entre números primos y compuestos:

- Los números primos corresponden a la conciencia HD: son no-lineales, cualitativos, descriptivos, sintéticos e inanalizables. Están en un nivel profundo y hacen referencia a sí mismos. A los números primos se les suele denominar "el código de Dios" porque se considera que están en el nivel más primario y profundo.

- Los números compuestos corresponden a la conciencia HI: son lineales, cuantitativos, operativos, analizables y descomponibles. Están en un nivel superficial y hacen referencia (explícita o implícitamente) a los números primos. Son manifestaciones de combinaciones (tipo producto) de números primos. Son tanto más superficiales cuanto más grandes son.

Los números son arquetipos. Los números primos son arquetipos primarios. Cuanto menor es un número primo, mayor es su profundidad como arquetipo y mayores son sus manifestaciones en los números compuestos. Los números compuestos son proyecciones o manifestaciones de los números primos.

Tratar de capturar el patrón de los números primos es imposible porque ese patrón pertenece al HD y su captura requiere del HI, y esto no es posible porque el HD está en un nivel superior al HI.

El patrón de los números primos no puede ser superficial (tipo "conciencia HI"), sino profundo (tipo "conciencia HD"). No puede ser de tipo operativo y cuantitativo, sino que tiene que ser forzosamente descriptivo y cualitativo. De hecho, ya existe un patrón descriptivo, que es la propia definición de número primo.

Lo superficial puede expresarse en términos de lo profundo, pero no al revés: lo profundo no puede expresarse en términos de lo superficial. Sería una contradicción que los números primos se pudieran expresar en términos de relaciones aritméticas o algebraicas a partir de sí mismos o de los números compuestos, que son manifestaciones de los primos.

- La dualidad álgebra – geometría.
  En matemática, los dos modos de conciencia se reflejan en la dualidad álgebra-geometría, en donde el álgebra corresponde a la conciencia HI y la geometría a la

conciencia HD. La que podemos denominar "conciencia matemática" surge cuando álgebra y geometría están conectadas.

El teorema de Pitágoras desempeña un papel fundamental en la conexión entre álgebra y geometría. En efecto, si tenemos la expresión $x+y = z$, entonces existe un triángulo rectángulo de catetos $\sqrt{x}$, $\sqrt{y}$ e hipotenusa $\sqrt{z}$. Es decir, que en la suma –la operación más fundamental de la matemática– está implícito el teorema de Pitágoras. De ahí su enorme importancia como conector universal entre álgebra y geometría:

- De la geometría se pasa al álgebra elevando al cuadrado los números que representan las longitudes de los lados del triángulo rectángulo.
- Del álgebra se pasa a la geometría transformando los números de una suma en raíces cuadradas.

El teorema de Pitágoras representa la "conciencia matemática": la conexión entre álgebra y geometría, es decir, la unión de los dos modos de conciencia.

Como la conciencia HD es superior a la conciencia HI, y como la geometría es conciencia HD y el álgebra es conciencia HI, la geometría se sitúa en un nivel superior al álgebra, por lo que el álgebra debería ser una particularización o manifestación de la geometría.

Por lo tanto, el patrón de los números primos no puede ser de tipo algebraico porque el álgebra es inferior a la geometría. Es desde el nivel superior de la geometría donde quizás se podría encontrar el patrón de los números primos.

La estrategia a seguir: los principios generales

Los múltiples intentos a lo largo de la historia que han tratado de encontrar el patrón de los números primos han estudiado su distribución desde el punto de vista analítico, algebraico, aritmético y cuantitativo. Pero para entender los números primos no debemos analizar los números primos, sino situarnos en un nivel superior. No se trata de buscar relaciones horizontales entre los números primos sino de elevarse lo más posible y buscar principios o leyes generales o universales que se proyecten o manifiesten como números primos. Los principios que podrían aplicarse son los siguientes:

- El principio de causalidad descendente.
  Este principio universal afirma que todo efecto proviene de un nivel más profundo. Que lo superficial es una manifestación de lo profundo. Y que desde lo superficial no es posible expresar lo profundo.

  El conjunto de los números primos hay que considerarlos a nivel holístico. Hay que considerarlos como un todo y en el que todos los números primos estén relacionados desde un nivel superior.

- El principio de simplicidad.
  Puesto que los números primos son el fundamento de todos los números naturales, su

estructura debe ser necesariamente simple, pues lo simple está asociado a lo profundo y a la conciencia.

El principio de simplicidad ha sido establecido de dos formas:

1. El principio de la navaja de Occam: ante diversas teorías que traten de explicar un fenómeno, hay que elegir la más simple.

2. El principio de Einstein, también denominado "navaja de Einstein". Este principio se basa en una frase atribuida al famoso científico: "Todo debería hacerse del modo más simple posible, pero no más simple".

   Esta frase ha sido objeto de polémica, pues se ha discutido mucho sobre su significado. Por ejemplo, se afirma que es contradictoria, pues si algo se ha hecho lo más simple posible, no puede hacerse aún más simple. Otros afirman que la frase debería decir "Todo debería hacerse del modo más simple posible, pero no demasiado simple".

   Seguramente, Einstein se refería a que la simplicidad tiene sus límites. Que no se debe ir más allá de la esencia conceptual de algo. Cuando se sobrepasa este límite, se entra en el campo puramente superficial, formal, mecánico o sintáctico, con pérdida de la semántica. Por ejemplo, un martillo puede hacerse más simple eliminando su cabeza, pero entonces deja de ser martillo, pues se pierde su esencia.

   Un ejemplo paradigmático es la lógica binaria, definida operativamente por tres conceptos: negación ($\neg$p), conjunción (p$\wedge$q) y disyunción (p$\vee$q). Sin embargo, es posible definir una operación aún más simple mediante la barra de Sheffer: "ni *p* ni *q*" (*p*|*q*) a partir de la cual se pueden definir las operaciones lógicas. Esto conduce, paradójicamente, a una mayor complejidad:

   $$\neg p = p|p \qquad p \vee q = (p|q) \mid (p|q)$$
   $$p \wedge q = ((p|p)|(q|q)|(p|p)|(q|q)) \mid ((p|p)|(q|q)|(p|p)|(q|q))$$

- El principio de dualidad.
  Este principio afirma que, en el mundo manifestado, "Todo es dual, todo tiene dos polos". A nivel profundo (no manifestado) no hay dualidad. La dualidad se manifiesta principalmente como simetría, como complementariedad o como conceptos opuestos.

  La dualidad es un principio clave para entender la realidad. La clave de toda teoría reside en la identificación de las dualidades. La unificación de teorías se basa en encontrar sus dualidades y unificarlas. Esto es especialmente útil en física, donde las dualidades se unifican en conceptos como espacio-tiempo, masa-energía y onda-corpúsculo. Lo que se trata es de armonizar las dualidades y buscar conceptos superiores.

  Existe dualidad entre los números primos y los compuestos. Pero también los números primos deben tener una naturaleza dual. Debe haber primos opuestos, simétricos o

complementarios. De hecho, hay primos simétricos o duales, que son los primos gemelos (los primos que difieren en 2). El interés por los números primos gemelos se debe a que simbolizan la conciencia, la unión de los opuestos.

Esta dualidad también debe existir para los números compuestos.

- El paradigma fractal.
  Este es un principio universal: hay un conjunto de principios generales que se manifiestan en todos los niveles: en el macrocosmos, en el microcosmos, en lo interno (la mente) y en lo externo (la naturaleza).

  La definición de número primo es muy simple, pero su distribución es aparentemente muy compleja. Pero puede ocurrir lo mismo que con los fractales, que tienen leyes generadoras simples pero que aplicadas recursivamente producen gran complejidad. El paradigma de este enfoque es el conjunto de Mandelbrot, en el que una ecuación simple ($z = z^2+c$) en el plano complejo, aplicada recursivamente, produce una estructura infinitamente compleja.

La estrategia a seguir para intentar encontrar el patrón de los números primos la vamos a basar concretamente en:

1. El patrón envolvente $4k\pm1$.
   Este patrón tiene la ventaja de que cumple el principio de simplicidad de Einstein –la simplicidad máxima sería el patrón $2k+1$–, así como el principio de dualidad: los números duales ($4k-1$ y $4k+1$) difieren en 2. Además incluye a todos los números impares, proporcionando un entorno que permite relacionar los números primos y los compuestos.

2. El teorema de Pitágoras.
   El teorema de Pitágoras se considera el teorema más fundamental de la matemática porque conecta álgebra y geometría. Es un teorema profundo, un teorema de la conciencia. Puesto que los números primos pertenecen al reino de lo profundo deben tener una relación estrecha con el teorema de Pitágoras.

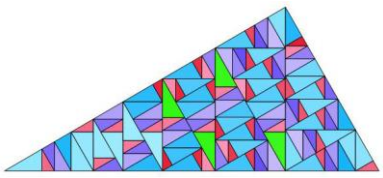
   El teorema de Pitágoras cumple las propiedades requeridas de:

   - Causalidad descendente. El teorema de Pitágoras conecta la geometría con el álgebra, en donde el álgebra es una manifestación de la geometría.

   - Simplicidad. El triángulo rectángulo es la forma geométrica más simple que hay. Toda forma geométrica 2D se puede descomponer en triángulos. A su vez, todo triángulo se puede descomponer en dos triángulos rectángulos.

   - Dualidad. El teorema de Pitágoras, expresado como suma de cuadrados ($x^2+y^2 = z^2$) tiene su dual como diferencia de cuadrados ($z^2-y^2 = x^2$), en la que está implícito el producto: $z^2-y^2 = (z+y)(z-y)$. Esta dualidad también se manifiesta en los términos primero y tercero de las ternas pitagóricas, que tienen la forma $(a^2-b^2, 2ab, a^2+b^2)$.

- Fractalidad. La fractalidad se manifiesta al dividir un triángulo rectángulo en dos triángulos rectángulos semejantes, y aplicando este mecanismo de forma recursiva (ver figura).



La fractalidad de un triángulo rectángulo

Propiedades de las Expresiones Pitagóricas

Producto de dos números que son suma de cuadrados

Si dos números naturales se pueden expresar como suma de dos cuadrados, $a_1^2+b_1^2$ y $a_2^2+b_2^2$, entonces su producto también se puede expresar como suma de dos cuadrados, de dos formas:

1. $(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + a_2b_1)^2$
2. $(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 + b_1b_2)^2 + (a_1b_2 - a_2b_1)^2$

Por ejemplo:

1. $65 = 5\times13 = (1^2 + 2^2)\,(2^2 + 3^2) = (2 - 6)^2 + (3 + 4)^2 = 4^2 + 7^2$
2. $65 = 5\times13 = (1^2 + 2^2)\,(2^2 + 3^2) = (2 + 6)^2 + (3 - 4)^2 = 8^2 + 1^2$

En el caso de que los dos números a multiplicar sean iguales, solo tiene sentido aplicar la primera fórmula, pues la segunda conduce a una identidad:

1. $(a^2 + b^2)(a^2 + b^2) = (a^2 - b^2)^2 + (ab + ab)^2 = (a^2 - b^2)^2 + (2ab)^2$
2. $(a^2 + b^2)(a^2 + b^2) = (a^2 + b^2)^2 + (ab - ab)^2 = (a^2 + b^2)^2$

Por ejemplo, $25 = 5\times5 = (1^2+2^2)(1^2+2^2) = (1^2-2^2)^2 + (2\times2)^2 = 3^2 + 4^2$

Todo número compuesto es una diferencia de cuadrados

Todo número natural compuesto n del tipo $x\times y$, en donde $x<y$, se puede expresar como diferencia entre dos cuadrados: $a^2 - b^2$. En efecto, haciendo $x = (a-b)$ e $y = (a+b)$, se tiene:

$$a = (x+y)/2 \qquad b = (y-x)/2 \qquad n = x\times y = (a+b)\times(a-b) = a^2 - b^2$$

Es decir, $n = x\times y = ((x+y)/2)^2 - ((y-x)/2)^2$

Para que a y b sean enteros, x e y deben de tener la misma paridad. Por ejemplo:

$n = 5\times37$, $a = (37+5)/2 = 21$, $b = (37-5)/2 = 16$, $n = 21^2 - 16^2$
$n = 15\times9$, $a = (15+9)/2 = 12$, $b = (15-9)/2 = 3$, $n = 12^2 - 3^2$
$n = 4\times14$, $a = (14+4)/2 = 18/2 = 9$, $b = (14-4)/2 = 10/2 = 5$, $n = 9^2 - 5^2$

Si no tienen la misma paridad, entonces se tiene por ejemplo

$$n = 4\times13,\ a = (13+4)/2 = 17/2,\ b = (13-4)/2 = 9/2,\ n = (17/2)^2 - (9/2)^2$$

Versión inversa: Si un número natural n se puede expresar como la diferencia entre dos cuadrados, $n = a^2-b^2$, entonces n es un número compuesto: $n = x\times y$, siendo $x = (a-b)$ e $y = (a+b)$, es decir, $n = (a+b)\times(a-b)$.

En el caso de que $a-b = 1$, es decir, si a y b son números consecutivos ($a = b+1$), tenemos que $n = a^2-b^2 = (a+b)\times(a-b) = a+b$, que es siempre un número impar. Por ejemplo, $7^2-6^2 = 6+7 = 13$, $8^2-7^2 = 8+7 = 15$. Por lo tanto, todo número impar se puede expresar como la diferencia entre los cuadrados de dos números consecutivos.

Producto de dos números que son diferencia de cuadrados

Dados dos números naturales que pueden expresarse como diferencia de dos cuadrados, $a_1^2-b_1^2$ y $a_2^2-b_2^2$, entonces su producto se puede expresar como diferencia de dos cuadrados, también (como en el caso de la suma de cuadrados) de dos formas:

1. $(a_1^2-b_1^2)(a_2^2-b_2^2) = (a_1a_2 + b_1b_2)^2 - (a_1b_2 + a_2b_1)^2$
2. $(a_1^2-b_1^2)(a_2^2-b_2^2) = (a_1a_2 - b_1b_2)^2 - (a_1b_2 - a_2b_1)^2$

Por ejemplo:

$$21 = 3\times7 = (2^2-1^2)\,(4^2-3^2) = (8+3)^2 - (6+4)^2 = 11^2-10^2$$
$$21 = 3\times7 = (2^2-1^2)\,(4^2-3^2) = (8-3)^2 - (6-4)^2 = 5^2-2^2$$

En el caso de que los dos números sean iguales, solo tiene sentido aplicar la primera fórmula, pues la segunda conduce a una identidad:

1. $(a^2 - b^2)(a^2 - b^2) = (a^2 + b^2)^2 - (ab + ab)^2 = (a^2 + b^2)^2 - (2ab)^2$
2. $(a^2 - b^2)(a^2 - b^2) = (a^2 - b^2)^2 - (ab - ab)^2 = (a^2 - b^2)^2$

Por ejemplo, $49 = 7\times7 = (4^2-3^2)\,(4^2-3^2) = (4^2+3^2)^2 - 24^2 = 25^2 - 24^2$

Producto de suma de cuadrados por diferencia de cuadrados

Dados dos números naturales que pueden expresarse como suma y diferencia de dos cuadrados, respectivamente, $n_1 = a_1^2+b_1^2$ y $n_2 = a_2^2-b_2^2$, entonces su producto también se puede expresar como diferencia de dos cuadrados:

$$(a_1^2+b_1^2)(a_2^2-b_2^2) = ((a_1^2 + b_1^2 + a_2^2 - b_2^2)/2)^2 - ((a_1^2 + b_1^2 - a_2^2 + b_2^2)/2)^2$$

Esta expresión surge de la ecuación $(a_1^2+b_1^2)(a_2^2-b_2^2) = x\times y$, haciendo $x = a_1^2+b_1^2$ e $y = a_2^2-b_2^2$.

Si n_1 y n_2 son ambos impares, entonces a_1 y b_1, así como a_2 y b_2, tienen distinta paridad. En consecuencia, resulta una diferencia de cuadrados entre enteros. Por ejemplo: $7\times29 = (4^2-3^2)\times(2^2+5^2) = 18^2-11^2$

Números pares vs. expresiones pitagóricas

El número 2 se puede expresar como la expresión pitagórica positiva 1^2+1^2. Las potencias 2^n son también expresiones pitagóricas positivas. En general:

Si n es par, $2^n = (2^{n/2})^2$.
Si n es impar, $2^n = (2^{(n-1)/2})^2 + (2^{(n-1)/2})^2$

Un número impar es de la forma $2^n k$, siendo $n\geq1$ y $k\geq1$ impar. El número k puede ser de tipo a^2, a^2+b^2 o a^2-b^2. Llamando $c = 2^{(n-1)/2}$, tenemos:

k	Valor de $2^n k$ si n par	Valor de $2^n k$ si n impar
a^2	$(2^{n/2}a)^2$	$(ac)^2 + (ac)^2$
a^2+b^2	$(2^{n/2}a)^2 + (2^{n/2}b)^2$	$((ac)^2-(bc)^2)^2 + ((bc)^2+(ac)^2)^2$
a^2-b^2	$(2^{n/2}a)^2 - (2^{n/2}b)^2$	$(2c^2+a^2-b^2)/2)^2 - (2c^2-a^2+b^2)/2)^2$

Puesto que a y b tienen distinta paridad, la última expresión es una diferencia de cuadrados de números no enteros.

La geometría de las expresiones pitagóricas equivalentes

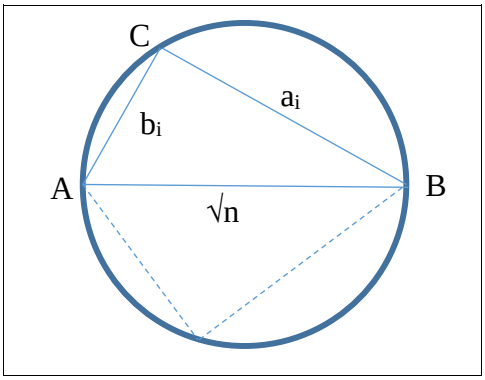
Cuando tenemos varias sumas de dos cuadrados de tipo $4k+1$, que corresponden a un mismo número compuesto,

$$n = a_1^2+b_1^2 = a_2^2+b_2^2 = \ldots = a_m^2+b_m^2$$

por ejemplo,

$$1105 = 4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2$$

entonces los vértices de los triángulos rectángulos de catetos a_i y b_i pertenecen a una circunferencia de diámetro $\sqrt{n}$ (ver figura).

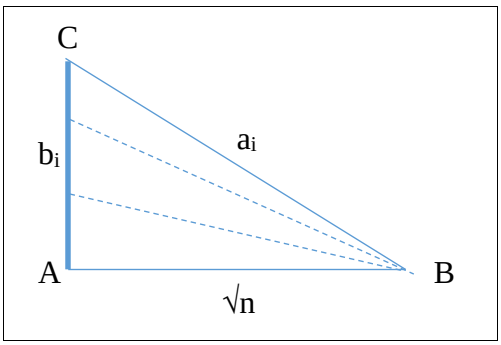


Cuando tenemos varias diferencias entre dos cuadrados, que corresponden a un mismo número compuesto,

$$n = a_1^2 - b_1^2 = a_2^2 - b_2^2 = \ldots = a_m^2 - b_m^2$$

por ejemplo,

$$885 = 37^2 - 22^2 = 91^2 - 86^2 = 149^2 - 146^2$$



si consideramos los triángulos rectángulos de base AB = $\sqrt{n}$, entonces todos los vértices C pertenecen a la recta perpendicular a AB que pasa por A (ver figura).

El Teorema de Fermat de la Suma de Cuadrados y su Dual

El Teorema de Fermat de la suma de cuadrados

Este teorema [9] [10] [11] afirma que todo número primo p de la forma $4k+1$, es decir, $p \equiv 1$ (módulo 4), se puede expresar como una suma única de dos cuadrados: $p = a^2+b^2$. Y viceversa: si un número primo se puede expresar como suma de cuadrados, entonces es de tipo $4k+1$. Por ejemplo,

$$13 = 4\times3 + 1 = 2^2 + 3^2 \qquad 17 = 4\times4 + 1 = 1^2 + 4^2 \qquad 29 = 4\times7 + 1 = 2^2 + 5^2$$

Los primeros números primos de este tipo son: 5, 13, 17, 29, 37, 41, 53, …

En este teorema hay que tener en cuenta las restricciones siguientes:

1. Los números a y b tienen que tener distinta paridad, porque si tuvieran la misma paridad, $p = a^2+b^2$ sería par y no sería primo.
2. Los números a y b no pueden ser iguales porque a^2+b^2 sería también par. Por lo tanto, podemos suponer que $a<b$.
3. Los números a y b tienen que ser coprimos, porque si tuvieran un factor común, entonces a^2+b^2 no sería primo porque sería múltiplo de ese factor.

Fermat enunció este teorema en una carta a Mersenne el 25 de Diciembre de 1640, razón por la cual se conoce a este teorema como "teorema de Navidad de Fermat". El teorema apareció en la publicación de 1670 del hijo de Fermat de las notas de su padre en su ejemplar de la Aritmética de Diofanto.

Euler afirmó en una carta a Christian Goldbach, el 12 de Abril de 1749, que lo había demostrado. En 1783 publicó una demostración completa, en la que utilizó el método del descenso infinito. Lagrange publicó una demostración en 1775, basada en formas cuadráticas. Esta última demostración fue simplificada por Gauss en sus *Disquisitiones Arithmeticae*. Dedekind proporcionó otras dos demostraciones basadas en los enteros gaussianos.

Este teorema fue calificado por G.H. Hardy como "uno de los más bellos de la aritmética" [12].

Los matemáticos están todavía hoy interesados en él por dos razones: 1) Por el papel que desempeña en la conexión entre álgebra y geometría; 2) Para intentar conseguir una demostración lo más simple posible y que ayude a comprender la verdadera naturaleza de los números primos.

Otros números que son sumas de cuadrados

Además de los primos tipo $4k+1$, hay otros números que pueden expresarse como suma de dos cuadrados a^2+b^2, pero que son compuestos, en dos casos:

1. Cuando esta descomposición no es única. Por ejemplo:

   $85 = 5\times17 = 2^2 + 9^2 = 6^2 + 7^2 \qquad 221 = 5^2 + 14^2 = 10^2 + 11^2$

2. Cuando a y b son los dos primeros elementos de una terna pitagórica (a, b, c), es decir, cuando existe un número c tal que $a^2+b^2 = c^2$. Por ejemplo,

   $3^2+4^2 = 5^2 \quad 5^2+12^2 = 13^2 \quad 8^2+15^2 = 17^2 \quad 20^2+21^2 = 29^2 \quad 12^2+35^2 = 37^2$

Estos dos tipos de números compuestos son también del tipo $4k+1$. En general, todo número impar n que se pueda expresar como suma de cuadrados es de tipo $4k+1$, como puede demostrarse fácilmente:

> En efecto, todo número cuadrado (2^2, 3^2, 4^2, 5^2, …) cumple que sus restos al dividirlos por 4 son 0 o 1. Por lo tanto,
>
> $a^2 \equiv 0$ o 1 (módulo 4) $\qquad b^2 \equiv 0$ o 1 (módulo 4)
> $n = a^2+b^2 \equiv 0$ o 1 o 2 (módulo 4)
>
> Pero $n \equiv 0$ o 2 (módulo 4) hay que descartarlos porque n sería par. Por lo tanto, solo queda que $n \equiv 1$ (módulo 4).

Teorema dual del teorema de Navidad de Fermat

El teorema de Navidad de Fermat es un teorema verdaderamente notable porque relaciona los números primos impares tipo $4k+1$ (objetos cuya definición implica la multiplicación y la división) con la estructura aditiva de los números cuadrados. Al considerar los números cuadrados nos estamos "elevando" a la geometría, que está en un nivel superior al álgebra. De esta manera se simplifica notablemente la búsqueda de las relaciones entre los números naturales (los primos y los compuestos).

Por lo tanto, el teorema de Navidad de Fermat no es un teorema más de la teoría de números, sino el teorema más fundamental, pues conecta el álgebra y la geometría, revelando la estrecha conexión existente entre los números primos y el teorema de Pitágoras. Este teorema es equiparable en importancia al teorema fundamental de la aritmética.

No obstante, el teorema de Navidad de Fermat necesita ser complementado, pues es natural considerar la operación dual: la diferencia de cuadrados.

Sabemos, por el teorema de Navidad de Fermat, que si n es primo y de tipo $4k+1$, entonces es expresable de manera única como suma de dos cuadrados. Esta es la propiedad que caracteriza a los primos de la rama $4k+1$ de los números impares.

Si n es primo y es de tipo $4k-1$, entonces:

- No es expresable como suma de cuadrados, porque si lo fuera sería de tipo $4k+1$.
- No es expresable como diferencia de cuadrados, porque si lo fuera sería un número compuesto.

Por consiguiente, un número primo de tipo $4k-1$ no es expresable ni como suma ni como diferencia de cuadrados, obviando la relación trivial de que todos los impares son la diferencia entre los cuadrados de dos números consecutivos. Otra manera de decirlo es que un número primo de tipo $4k-1$ es solo expresable de manera trivial, es decir, como diferencia entre los cuadrados de dos números consecutivos. Esta es la propiedad fundamental que caracteriza a los primos de la rama $4k-1$ de los números impares.

Los primeros números primos de este tipo son: 3, 7, 11, 19, 23, 31, 43, …

Tabla de Expresiones Pitagóricas de los Números Impares. Propiedades

Haciendo uso del aspecto experimental de la teoría de números, se ha generado (mediante un programa de ordenador) la tabla de expresiones pitagóricas de los números impares (hasta el 601), con sus dos ramas ($4k-1$ y $4k+1$). (Ver Apéndice.)

- Los números primos aparecen sombreados.
- Cada expresión pitagórica va acompañada por el número asociado a su expresión pitagórica dual y la letra A o B, que indica el tipo $4k-1$ y $4k+1$, respectivamente.
- No se han considerado las expresiones pitagóricas triviales, es decir, la diferencia de cuadrados entre dos números consecutivos, aunque sí en los duales. Por ejemplo, la expresión dual de 3^2+4^2 es 4^2-3^2, que es trivial.

En la tabla aparecen expresiones pitagóricas duales (a^2-b^2 y a^2+b^2), es decir, que forman los extremos de una terna pitagórica. El número a^2-b^2 es siempre compuesto porque equivale al producto $(a+b)(a-b)$, a menos que $a-b = 1$, en cuyo caso puede ser primo o compuesto. El número a^2+b^2 puede ser primo o compuesto. Estas expresiones reflejan el teorema de Navidad de Fermat y su dual, así como las propiedades mencionadas anteriormente.

Lo primero que se observa en la tabla es que la rama $4k+1$ es más compleja porque está más "poblada" por expresiones pitagóricas que la rama $4k-1$, que es más simple, aunque el número de primos en ambas ramas es más o menos el mismo.

Tipos de números impares

En la rama $4k-1$ hay dos tipos de números:

1. Los que se expresan mediante una o varias expresiones pitagóricas negativas. Son números compuestos de tipo $\text{par}^2-\text{impar}^2$. Por ejemplo,

   $15 = 4^2-1^2 \qquad 27 = 6^2-3^2 \qquad 135 = 12^2-3^2 = 16^2-11^2 = 24^2-21^2$

2. Los que no tienen ninguna expresión pitagórica asociada. Solo son expresables como diferencia entre los cuadrados de dos números consecutivos. Son números primos, también de tipo $\text{par}^2-\text{impar}^2$. Por ejemplo, $3 = 2^2-1^2$ y $7 = 4^2-3^2$.

En la rama $4k+1$ hay 5 tipos de números:

1. Los que se expresan solo mediante una expresión pitagórica positiva y que no son cuadrados perfectos. Son números primos de tipo $\text{impar}^2+\text{par}^2$. Por ejemplo, $5 = 1^2+2^2$ y $13 = 2^2+3^2$.

2. Los que se expresan mediante una sola expresión pitagórica positiva y que son cuadrados perfectos. Son números compuestos de tipo $\text{impar}^2+\text{par}^2$. Por ejemplo: $5^2 = 3^2+4^2$ y $13^2 = 5^2+12^2$.

3. Los que son cuadrados perfectos, pero que no son expresables ni como suma ni como resta de cuadrados. Son números compuestos de tipo impar^2. Por ejemplo, 3^2, 7^2 y 11^2.

4. Los que se expresan mediante una o varias expresiones pitagóricas positivas, acompañadas por una o varias expresiones pitagóricas negativas. Son números compuestos de tipo $\text{impar}^2\pm\text{par}^2$. Por ejemplo: $45 = 3^2+6^2 = 7^2-2^2 = 9^2-6^2$ y $65 = 1^2+8^2 = 4^2+7^2 = 9^2-4^2$.

5. Los que se expresan mediante una o varias expresiones pitagóricas negativas. Son números compuestos de tipo $\text{impar}^2-\text{par}^2$. Por ejemplo: $33 = 7^2-4^2$ y $105 = 11^2-4^2 = 13^2-8^2 = 19^2-16^2$.

Por lo tanto, desde el punto de vista pitagórico, hay 6 tipos de números impares. Estos 6 tipos se pueden resumir en el patrón $a^2\pm b^2$, donde a y b tienen distinta paridad, donde $a>b$ y donde b puede ser cero.

Ternas pitagóricas

Todas las expresiones pitagóricas que aparecen en la tabla están conectadas mediante ternas pitagóricas tipo $(a^2-b^2,\ 2ab,\ a^2+b^2)$.

Como a y b tienen distinta paridad, ab es par (tipo $2k$) y $2ab$ es de tipo $4k$ (múltiplo de 4). Es decir, el término medio de una terna pitagórica está entre $4k-1$ y $4k+1$, las dos ramas de los números impares. Por ejemplo, en (3, 4, 5) es 4×1, en (15, 8, 17) es 4×2, en (5, 12, 13) es 4×3,

etc.

Las ternas pitagóricas de la tabla son de dos tipos:

1. Horizontales.
   Las expresiones pitagóricas que aparecen en la rama $4k-1$ son todas del tipo $n_1 = a^2-b^2$, con a par y b impar. Tienen su dual $n_2 = a^2+b^2$ en la rama $4k+1$. Los valores de a son: 2, 4, 6, 8, 10, 12, etc. Los valores de b son $a-3$, $a-5$, $a-7$, $a-9$, etc., es decir, $b = a-k$ (o $k = a-b$), con $k = 3, 5, 7, 9, \ldots$

   Hay dos formas de ver estas infinitas expresiones pitagóricas: fijando k o fijando b. Si se fija k, tenemos las ternas pitagóricas

   $$(a^2-b^2,\ 2ab,\ a^2+b^2) \text{ con } b = a-k, \text{ con } a = 4, 6, 8, 10,\ldots$$

   Y si se fija b tenemos las expresiones

   $$(a^2-b^2,\ 2ab,\ a^2+b^2) \text{ con } a = 4, 6, 8, 10,\ldots$$

   Ejemplo con $b = 1$ ($k = a-b$):

n_1	n_2
$3 = 2^2-1^2$ (primo)	$5 = 2^2+1^2$ (primo)
$15 = 4^2-1^2$ (compuesto)	$17 = 4^2+1^2$ (primo)
$35 = 6^2-1^2$ (compuesto)	$37 = 6^2+1^2$ (primo)
$63 = 8^2-1^2$ (compuesto)	$65 = 8^2+1^2$ (compuesto)
$99 = 10^2-1^2$ (compuesto)	$101 = 10^2+1^2$ (primo)

   Este ejemplo corresponde precisamente al caso de números gemelos (los que difieren en 2).

   Ejemplo con $k = 3$ ($b = a-k$):

n_1	n_2
$15 = 4^2-1^2$ (compuesto)	$17 = 4^2+1^2$ (primo)
$27 = 6^2-3^2$ (compuesto)	$45 = 6^2+3^2$ (compuesto)
$39 = 8^2-5^2$ (compuesto)	$89 = 8^2+5^2$ (primo)
$51 = 10^2-7^2$ (compuesto)	$149 = 10^2+7^2$ (primo)
$63 = 12^2-9^2$ (compuesto)	$223 = 12^2+9^2$ (primo)

2. Verticales.
   En la rama $4k+1$, las expresiones pitagóricas duales son $n_1 = a^2-b^2$, con a impar y b par y $n_2 = a^2+b^2$ en la propia rama $4k+1$. Los valores posibles de a son: 3, 5, 7, 9, 11, 13, etc. Los valores de b son $a-3$, $a-5$, $a-7$, $a-9$, etc., es decir, $b = a-k$ (o $k = a-b$), con $k = 3, 5, 7, 9, \ldots$

   Como en el caso anterior, hay dos formas de ver estas expresiones pitagóricas, que son

infinitas: fijando *k* o fijando *b*. Si se fija *k*, tenemos las expresiones

$(a^2–b^2, 2ab, a^2+b^2)$ con $b = a–k$, con $a = 5, 7, 9, 11,\ldots$

Y si se fija *b* tenemos las expresiones

$(a^2–b^2, 2ab, a^2+b^2)$ con $a = 5, 7, 9, 11,\ldots$

Ejemplo con $b = 2$ ($k = a–b$):

n_1	n_2
$5 = 3^2–2^2$ (primo)	$13 = 3^2+2^2$ (primo)
$21 = 5^2–2^2$ (compuesto)	$29 = 5^2+2^2$ (primo)
$45 = 7^2–2^2$ (compuesto)	$53 = 7^2+2^2$ (primo)
$77 = 9^2–2^2$ (compuesto)	$85 = 9^2+2^2$ (compuesto)
$117 = 11^2–2^2$ (compuesto)	$125 = 11^2+2^2$ (compuesto)
$165 = 13^2–2^2$	$173 = 13^2+2^2$ (primo)

Ejemplo con k = 3 (b = a–k):

n_1	n_2
$21 = 5^2–2^2$ (compuesto)	$29 = 5^2+2^2$ (primo)
$33 = 7^2–4^2$ (compuesto)	$65 = 7^2+4^2$ (compuesto)
$48 = 9^2–6^2$ (compuesto)	$117 = 9^2+6^2$ (compuesto)
$117 = 11^2–8^2$ (compuesto)	$185 = 11^2+8^2$ (compuesto)
$69 = 13^2–10^2$ (compuesto)	$269 = 13^2+10^2$ (primo)

Sistema Tradicional vs. Sistema Pitagórico

Con la ayuda de la suma de cuadrados y su dual (la diferencia de cuadrados), es decir, considerando las expresiones pitagóricas positivas y negativas, hemos obtenido un marco conceptual basado en la simplicidad, la dualidad y la fractalidad. Si comparamos el sistema tradicional (T), basado en los números primos y los compuestos (como producto de primos), con el sistema pitagórico (P), basado en la suma y resta de cuadrados, tenemos las siguientes diferencias y analogías:

- Estructura de los números fundamentales o primarios.
  T: Son los números primos, que es una estructura desordenada, sin patrón conocido: (2, 3, 5, 7, 11, …).
  P: Son los cuadrados de los números naturales, que es una estructura ordenada: (1^2, 2^2, 3^2, 4^2, 5^2,…).

- Operaciones.
  T: Multiplicación y división.
  P: Suma y resta de cuadrados. Son operaciones más sencillas que la multiplicación y

división. Proporcionan un marco más rico y flexible en el que es posible deducir con más facilidad las propiedades de los números (primos y compuestos).

- Teorema fundamental.
  T: Teorema fundamental de la aritmética: todo número natural tiene una descomposición única en sus factores primos.
  P: El teorema fundamental es el teorema de Navidad de Fermat y su dual.

- Descripción de los números primos.
  T: Los números primos son los que solo son divisibles por sí mismos y por la unidad.
  P: Hay una descripción pitagórica. Un primo de tipo $4k+1$ es solo expresable como suma única de cuadrados. Un primo de tipo $4k-1$ es inexpresable como suma y como resta de cuadrados. Solo es expresable como diferencia entre los cuadrados de dos números consecutivos, como todos los números impares.

- Números compuestos.
  T: Un número compuesto es una expresión única como producto de números primos.
  P: Un número compuesto puede tener múltiples expresiones, como varias sumas de cuadrados y/o como una o varias diferencias de cuadrados.

  En general, cuanto mayor es el número compuesto, mayor es el número de expresiones pitagóricas posibles para representarlo. Esto supone un marco de flexibilidad que el sistema tradicional no tiene.

- El número 1.
  T: El número 1 no se considera primo. No desempeña ningún papel. Es el elemento neutro de la multiplicación: $n \times 1 = n$.
  P: Es un número esencial como componente de expresiones pitagóricas tipo a^2-1^2 y a^2+1^2. Es el único número cuyo cuadrado es igual a sí mismo: $1^2 = 1$.

- La singularidad del 2.
  T: El 2 es el único número primo par.
  P: El 2 es el único número que es la suma de dos cuadrados iguales: $2 = 1^2+1^2$. No es un primo gaussiano porque $2 = (1+i)(1-i)$.

- Elementos triviales.
  T: Hay dos divisores triviales: el propio número (n) y la unidad (1).
  P: La diferencia entre los cuadrados de dos enteros consecutivos.

- Elementos del test de primalidad.
  T: Los divisores no triviales.
  P: Las expresiones pitagóricas de suma y resta de cuadrados.

- Test de primalidad.
  T: Lo descriptivo implica lo operativo. La descripción tradicional de los números primos –un número primo solo es divisible por sí mismo y por la unidad– proporciona un método para averiguar si un número n es primo. Se buscan los divisores propios de n. Si no se encuentran, entonces n es primo. En caso contrario, es compuesto.

P: La descripción pitagórica también proporciona un método para averiguar si un número n (impar) es primo:

1. Si n es de tipo $4k+1$ y no es un cuadrado perfecto, se buscan las expresiones equivalentes de n que sean suma de cuadrados. Si solo se encuentra una, n es primo. En caso contrario, n es compuesto.
2. Si n es de tipo $4k-1$, se buscan las expresiones (no triviales) equivalentes de n que sean resta de cuadrados. Si no se encuentran, n es primo. En caso contrario, n es compuesto.

- Factorización.
  T: Es de tipo lineal, un método de la conciencia HI. Para saber si un número es primo basta con dividirlo entre todos los números primos inferiores a su raíz cuadrada. La razón de esto es porque los factores operan en pares. Si un número n tiene un factor $>\sqrt{n}$, también tiene que tener otro factor $<\sqrt{n}$. Por ejemplo, $n = 35 = 5\times7$, $5<\sqrt{35}$ y $7>\sqrt{35}$.

  P: Es de tipo fractal descendente, un método de la conciencia HD. Hay dos casos:

  1. Si el número n es impar, se buscan dos posibles factores primos, que corresponden a una diferencia de cuadrados: $n = a^2-b^2 = (a+b)(a-b)$, en donde a y b tienen distinta paridad. A cada uno de estos dos factores (que son también impares) se vuelve a aplicar el mismo procedimiento, y así sucesivamente. Es una búsqueda dual en el sentido de que se buscan dos números a la vez en todos los pasos.

  2. Si el número n es par, se convierte a $2^m n_1$, siendo $m\geq1$ y n_1 impar. A n_1 se le aplica el procedimiento anterior.

Resumen y conclusiones

Hay dos categorías de números primos impares:

1) Los que pueden expresarse de manera única como suma de cuadrados y que no son cuadrados perfectos. Son de tipo $4k+1$. Esta propiedad corresponde al teorema de Navidad de Fermat.

2) Los que no pueden expresarse ni como suma de cuadrados ni como diferencia de cuadrados (excluyendo la resta trivial de los cuadrados de dos números consecutivos). Son de tipo $4k-1$. Esta propiedad corresponde al teorema dual del teorema de Navidad de Fermat.

Los números primos no tienen un patrón algebraico, sino un patrón cualitativo basado en estas dos propiedades fundamentales.

Hay varias razones para no considerar los primos tipo $4k+1$ como verdaderos números primos:

1. No son primos gaussianos.

2. Son expresables como suma de dos números compuestos (a^2 y b^2), lo que conceptualmente es una contradicción. Los números primos no deberían ser expresables, pues todos los demás números (los números compuestos) se construyen sobre ellos.

3. Tienen la misma forma que los números compuestos en los que aparecen varias sumas de cuadrados.

4. Hay una evidente asimetría entre las ramas $4k-1$ y $4k+1$, pues la rama $4k+1$ está más "poblada" y es más compleja que la $4k-1$:

    a) Desde el punto de vista de las expresiones pitagóricas, en la rama $4k-1$ hay 2 tipos de números, y en la rama $4k+1$ hay 5.
    b) Hay expresiones pitagóricas positivas solo en la rama $4k+1$.
    c) Hay más expresiones pitagóricas negativas en la rama $4k-1$ que en la rama $4k-1$.
    d) Hay ternas pitagóricas en la rama $4k+1$, mientras que no hay ninguna en la rama $4k-1$.

    Al haber más manifestaciones en la rama $4k+1$, esto hace sugerir que está en un nivel inferior a la rama $4k-1$, es decir, que esta rama sería más fundamental.

Por lo tanto, si consideramos los primos de tipo $4k+1$ como números compuestos, solo nos quedan los primos tipo $4k-1$, que tienen la propiedad de ser inexpresables y que trascienden los opuestos (la suma y resta de cuadrados), situándose en un nivel más profundo, trans-pitagórico. Esto coincide con la filosofía de que desde lo superficial no se puede acceder a lo profundo.

En definitiva, no hay nada extraño ni misterioso ni complejo en el tema de los números primos. Al contrario, es algo fundamentalmente simple por su estrecha relación con el teorema de Pitágoras. La clave de la comprensión de los números primos reside en la suma/resta de cuadrados, es decir, las formas duales del teorema de Pitágoras. El teorema de Pitágoras es el teorema más fundamental de la matemática. El teorema de Pitágoras es un teorema de la conciencia, el Santo Grial de la matemática.

Apéndice

Tabla de expresiones pitagóricas de los números impares

Nº A	Tipo	Expresión y su dual	Nº B	Tipo	Expresión y su dual
3	Primo		**5**	Primo	1^2+2^2 **3** (A)
7	Primo		**9**	3^2	
11	Primo		**13**	Primo	2^2+3^2 **5** (B)

15	3*5	$4^2–1^2$ **17** (B)	**17**	Primo	1^2+4^2 **15** (A)
19	Primo		**21**	3*7	$5^2–2^2$ **29** (B)
23	Primo		**25**	5^2	3^2+4^2 **7** (A)
27	3^3	$6^2–3^2$ **45** (B)	**29**	Primo	2^2+5^2 **21** (B)
31	Primo		**33**	3*11	$7^2–4^2$ **65** (B)
35	5*7	$6^2–1^2$ **37** (B)	**37**	Primo	1^2+6^2 **35** (A)
39	3*13	$8^2–5^2$ **89** (B)	**41**	Primo	4^2+5^2 **9** (B)
43	Primo		**45**	3^2*5	3^2+6^2 **27** (A) $7^2–2^2$ **53** (B) $9^2–6^2$ **117** (B)
47	Primo		**49**	7^2	
51	3*17	$10^2–7^2$ **149** (B)	**53**	Primo	2^2+7^2 **45** (B)
55	5*11	$8^2–3^2$ **73** (B)	**57**	3*19	$11^2–8^2$ **185** (B)
59	Primo		**61**	Primo	5^2+6^2 **11** (A)
63	3^2*7	$8^2–1^2$ **65** (B) $12^2–9^2$ **225** (B)	**65**	5*13	1^2+8^2 **63** (A) 4^2+7^2 **33** (B) $9^2–4^2$ **97** (B)
67	Primo		**69**	3*23	$13^2–10^2$ **269** (B)
71	Primo		**73**	Primo	3^2+8^2 **55** (A)
75	$3*5^2$	$10^2–5^2$ **125** (B) $14^2–11^2$ **317** (B)	**77**	7*11	$9^2–2^2$ **85** (B)
79	Primo		**81**	3^4	$15^2–12^2$ **369** (B)
83	Primo		**85**	5*17	2^2+9^2 **77** (B) 6^2+7^2 **13** (B) $11^2–6^2$ **157** (B)
87	3*29	$16^2–13^2$ **425** (B)	**89**	Primo	5^2+8^2 **39** (A)
91	7*13	$10^2–3^2$ **109** (B)	**93**	3*31	$17^2–14^2$ **485** (B)
95	5*19	$12^2–7^2$ **193** (B)	**97**	Primo	4^2+9^2 **65** (B)

99	3^2*11	$10^2–1^2$ **101** (B) $18^2–15^2$ **549** (B)	**101**	Primo	1^2+10^2 **99** (A)
103	Primo		**105**	3*5*7	$11^2–4^2$ **137** (B) $13^2–8^2$ **233** (B) $19^2–16^2$ **617** (B)
107	Primo		**109**	Primo	3^2+10^2 **91** (A)
111	3*37	$20^2–17^2$ **689** (B)	**113**	Primo	7^2+8^2 **15** (A)
115	5*23	$14^2–9^2$ **277** (B)	**117**	3^2*13	6^2+9^2 **45** (B) $11^2–2^2$ **125** (B) $21^2–18^2$ **765** (B)
119	7*17	$12^2–5^2$ **169** (B)	**121**	11^2	
123	3*41	$22^2–19^2$ **845** (B)	**125**	5^3	2^2+11^2 **117** (B) 5^2+10^2 **75** (A) $15^2–10^2$ **325** (B)
127	Primo		**129**	3*43	$23^2–20^2$ **929** (B)
131	Primo		**133**	7*19	$13^2–6^2$ **205** (B)
135	3^3*5	$12^2–3^2$ **153** (B) $16^2–11^2$ **377** (B) $24^2–21^2$ **1017** (B)	**137**	Primo	4^2+11^2 **105** (B)
139	Primo		**141**	3*47	$25^2–22^2$ **1109** (B)
143	11*13	$12^2–1^2$ **145** (B)	**145**	5*29	1^2+12^2 **143** (A) 8^2+9^2 **17** (B) $17^2–12^2$ **433** (B)
147	$3*7^2$	$14^2–7^2$ **245** (B) $26^2–23^2$ **1205** (B)	**149**	Primo	7^2+10^2 **51** (A)
151	Primo		**153**	3^2*17	3^2+12^2 **135** (A) $13^2–4^2$ **185** (B) $27^2–24^2$ **1305** (B)
155	5*31	$18^2–13^2$ **493** (B)	**157**	Primo	6^2+11^2 **85** (B)
159	3*53	$28^2–25^2$ **1409** (B)	**161**	7*23	$15^2–8^2$ **289** (B)

163	Primo		**165**	3*5*11	$13^2–2^2$ **173** (B) $19^2–14^2$ **557** (B) $29^2–26^2$ **1517** (B)
167	Primo		**169**	13^2	5^2+12^2 **119** (A)
171	3^2*19	$14^2–5^2$ **221** (B) $30^2–27^2$ **1629** (B)	**173**	Primo	2^2+13^2 **165** (B)
175	5^2*7	$16^2–9^2$ **337** (B) $20^2–15^2$ **625** (B)	**177**	3*59	$31^2–28^2$ **1745** (B)
179	Primo		**181**	Primo	9^2+10^2 **19** (A)
183	3*61	$32^2–29^2$ **1865** (B)	**185**	5*37	4^2+13^2 **153** (B) 8^2+11^2 **57** (B) $21^2–16^2$ **697** (B)
187	11*17	$14^2–3^2$ **205** (B)	**189**	3^3*7	$15^2–6^2$ **261** (B) $17^2–10^2$ **389** (B) $33^2–30^2$ **1989** (B)
191	Primo		**193**	Primo	7^2+12^2 **95** (A)
195	3*5*13	$14^2–1^2$ **197** (B) $22^2–17^2$ **773** (B) $34^2–31^2$ **2117** (B)	**197**	Primo	1^2+14^2 **195** (A)
199	Primo		**201**	3*67	$35^2–32^2$ **2249** (B)
203	7*29	$18^2–11^2$ **445** (B)	**205**	5*41	3^2+14^2 **187** (A) 6^2+13^2 **133** (B) $23^2–18^2$ **853** (B)
207	3^2*23	$16^2–7^2$ **305** (B) $36^2–33^2$ **2385** (B)	**209**	11*19	$15^2–4^2$ **241** (B)
211	Primo		**213**	3*71	$37^2–34^2$ **2525** (B)
215	5*43	$24^2–19^2$ **937** (B)	**217**	7*31	$19^2–12^2$ **505** (B)
219	3*73	$38^2–35^2$ **2669** (B)	**221**	13*17	5^2+14^2 **171** (A) 10^2+11^2 **21** (B) $15^2–2^2$ **229** (B)

223	Primo		**225**	3^2*5^2	9^2+12^2 **63** (A) 17^2-8^2 **353** (B) 25^2-20^2 **1025** (B) 39^2-36^2 **2817** (B)
227	Primo		**229**	Primo	2^2+15^2 **221** (B)
231	3*7*11	16^2-5^2 **281** (B) 20^2-13^2 **569** (B) 40^2-37^2 **2969** (B)	**233**	Primo	8^2+13^2 **105** (B)
235	5*47	26^2-21^2 **1117** (B)	**237**	3*79	41^2-38^2 **3125** (B)
239	Primo		**241**	Primo	4^2+15^2 **209** (B)
243	3^5	18^2-9^2 **405** (B) 42^2-39^2 **3285** (B)	**245**	$5*7^2$	7^2+14^2 **147** (A) 21^2-14^2 **637** (B) 27^2-22^2 **1213** (B)
247	13*19	16^2-3^2 **265** (B)	**249**	3*83	43^2-40^2 **3449** (B)
251	Primo		**253**	11*23	17^2-6^2 **325** (B)
255	3*5*17	16^2-1^2 **257** (B) 28^2-23^2 **1313** (B) 44^2-41^2 **3617** (B)	**257**	Primo	1^2+16^2 **255** (A)
259	7*37	22^2-15^2 **709** (B)	**261**	3^2*29	6^2+15^2 **189** (B) 19^2-10^2 **461** (B) 45^2-42^2 **3789** (B)
263	Primo		**265**	5*53	3^2+16^2 **247** (A) 11^2+12^2 **23** (A) 29^2-24^2 **1417** (B)
267	3*89	46^2-43^2 **3965** (B)	**269**	Primo	10^2+13^2 **69** (B)
271	Primo		**273**	3*7*13	17^2-4^2 **305** (B) 23^2-16^2 **785** (B) 47^2-44^2 **4145** (B)
275	5^2*11	18^2-7^2 **373** (B) 30^2-25^2 **1525** (B)	**277**	Primo	9^2+14^2 **115** (A)

279	3^2*31	20^2–11^2 **521** (B) 48^2–45^2 **4329** (B)	**281**	Primo	5^2+16^2 **231** (A)
283	Primo		**285**	3*5*19	17^2–2^2 **293** (B) 31^2–26^2 **1637** (B) 49^2–46^2 **4517** (B)
287	7*41	24^2–17^2 **865** (B)	**289**	17^2	8^2+15^2 **161** (B)
291	3*97	50^2–47^2 **4709** (B)	**293**	Primo	2^2+17^2 **285** (B)
295	5*59	32^2–27^2 **1753** (B)	**297**	3^3*11	19^2–8^2 **425** (B) 21^2–12^2 **585** (B) 51^2–48^2 **4905** (B)
299	13*23	18^2–5^2 **349** (B)	**301**	7*43	25^2–18^2 **949** (B)
303	3*101	52^2–49^2 **5105** (B)	**305**	5*61	4^2+17^2 **273** (B) 7^2+16^2 **207** (A) 33^2–28^2 **1873** (B)
307	Primo		**309**	3*103	53^2–50^2 **5309** (B)
311	Primo		**313**	Primo	12^2+13^2 **25** (B)
315	3^2*5*7	18^2–3^2 **333** (B) 22^2–13^2 **653** (B) 26^2–19^2 **1037** (B) 34^2–29^2 **1997** (B) 54^2–51^2 **5517** (B)	**317**	Primo	11^2+14^2 **75** (A)
319	11*29	20^2–9^2 **481** (B)	**321**	3*107	55^2–52^2 **5729** (B)
323	17*19	18^2–1^2 **325** (B)	**325**	5^2*13	1^2+18^2 **323** (A) 6^2+17^2 **253** (B) 10^2+15^2 **125** (B) 19^2–6^2 **397** (B) 35^2–30^2 **2125** (B)
327	3*109	56^2–53^2 **5945** (B)	**329**	7*47	27^2–20^2 **1129** (B)
331	Primo		**333**	3^2*37	3^2+18^2 **315** (A) 23^2–14^2 **725** (B)

					$57^2–54^2$ **6165** (B)
335	5*67	$36^2–31^2$ **2257** (B)	**337**	Primo	9^2+16^2 **175** (A)
339	3*113	$58^2–55^2$ **6389** (B)	**341**	11*31	$21^2–10^2$ **541** (B)
343	7^3	$28^2–21^2$ **1225** (B)	**345**	3*5*23	$19^2–4^2$ **377** (B) $37^2–32^2$ **2393** (B) $59^2–56^2$ **6617** (B)
347	Primo		**349**	Primo	5^2+18^2 **299** (A)
351	3^3*13	$20^2–7^2$ **449** (B) $24^2–15^2$ **801** (B) $60^2–57^2$ **6849** (B)	**353**	Primo	8^2+17^2 **225** (B)
355	5*71	$38^2–33^2$ **2533** (B)	**357**	3*7*17	$19^2–2^2$ **365** (B) $29^2–22^2$ **1325** (B) $61^2–58^2$ **7085** (B)
359	Primo		**361**	19^2	
363	$3*11^2$	$22^2–11^2$ **605** (B) $62^2–59^2$ **7325** (B)	**365**	5*73	2^2+19^2 **357** (B) 13^2+14^2 **27** (A) $39^2–34^2$ **2677** (B)
367	Primo		**369**	3^2*41	12^2+15^2 **81** (B) $25^2–16^2$ **881** (B) $63^2–60^2$ **7569** (B)
371	7*53	$30^2–23^2$ **1429** (B)	**373**	Primo	7^2+18^2 **275** (A)
375	$3*5^3$	$20^2–5^2$ **425** (B) $40^2–35^2$ **2825** (B) $64^2–61^2$ **7817** (B)	**377**	13*29	4^2+19^2 **345** (B) 11^2+16^2 **135** (A) $21^2–8^2$ **505** (B)
379	Primo		**381**	3*127	$65^2–62^2$ **8069** (B)
383	Primo		**385**	5*7*11	$23^2–12^2$ **673** (B) $31^2–24^2$ **1537** (B) $41^2–36^2$ **2977** (B)
387	3^2*43	$26^2–17^2$ **965** (B) $66^2–63^2$ **8325** (B)	**389**	Primo	10^2+17^2 **189** (B)

391	17*23	$20^2–3^2$ **409** (B)	**393**	3*131	$67^2–64^2$ **8585** (B)
395	5*79	$42^2–37^2$ **3133** (B)	**397**	Primo	6^2+19^2 **325** (B)
399	3*7*19	$20^2–1^2$ **401** (B) $32^2–25^2$ **1649** (B) $68^2–65^2$ **8849** (B)	**401**	Primo	1^2+20^2 **399** (A)
403	13*31	$22^2–9^2$ **565** (B)	**405**	3^4*5	9^2+18^2 **243** (A) $21^2–6^2$ **477** (B) $27^2–18^2$ **1053** (B) $43^2–38^2$ **3293** (B) $69^2–66^2$ **9117** (B)
407	11*37	$24^2–13^2$ **745** (B)	**409**	Primo	3^2+20^2 **391** (A)
411	3*137	$70^2–67^2$ **9389** (B)	**413**	7*59	$33^2–26^2$ **1765** (B)
415	5*83	$44^2–39^2$ **3457** (B)	**417**	3*139	$71^2–68^2$ **9665** (B)
419	Primo		**421**	Primo	14^2+15^2 **29** (B)
423	3^2*47	$28^2–19^2$ **1145** (B) $72^2–69^2$ **9945** (B)	**425**	5^2*17	5^2+20^2 **375** (A) 8^2+19^2 **297** (B) 13^2+16^2 **87** (A) $21^2–4^2$ **457** (B) $45^2–40^2$ **3625** (B)
427	7*61	$34^2–27^2$ **1885** (B)	**429**	3*11*13	$23^2–10^2$ **629** (B) $25^2–14^2$ **821** (B) $73^2–70^2$ **10229** (B)
431	Primo		**433**	Primo	12^2+17^2 **145** (B)
435	3*5*29	$22^2–7^2$ **533** (B) $46^2–41^2$ **3797** (B) $74^2–71^2$ **10517** (B)	**437**	19*23	$21^2–2^2$ **445** (B)
439	Primo		**441**	3^2*7^2	$29^2–20^2$ **1241** (B) $35^2–28^2$ **2009** (B) $75^2–72^2$ **10809** (B)
443	Primo		**445**	5*89	2^2+21^2 **437** (B)

					11^2+18^2 **203** (A) 47^2-42^2 **3973** (B)
447	3*149	76^2-73^2 **11105** (B)	**449**	Primo	7^2+20^2 **351** (A)
451	11*41	26^2-15^2 **901** (B)	**453**	3*151	77^2-74^2 **11405** (B)
455	5*7*13	24^2-11^2 **697** (B) 36^2-29^2 **2137** (B) 48^2-43^2 **4153** (B)	**457**	Primo	4^2+21^2 **425** (B)
459	3^3*17	22^2-5^2 **509** (B) 30^2-21^2 **1341** (B) 78^2-75^2 **11709** (B)	**461**	Primo	10^2+19^2 **261** (B)
463	Primo		**465**	3*5*31	23^2-8^2 **593** (B) 49^2-44^2 **4337** (B) 79^2-76^2 **12017** (B)
467	Primo		**469**	7*67	37^2-30^2 **2269** (B)
471	3*157	80^2-77^2 **12329** (B)	**473**	11*43	27^2-16^2 **985** (B)
475	5^2*19	22^2-3^2 **493** (B) 50^2-45^2 **4525** (B)	**477**	3^2*53	6^2+21^2 **405** (B) 31^2-22^2 **1445** (B) 81^2-78^2 **12645** (B)
479	Primo		**481**	13*37	9^2+20^2 **319** (A) 15^2+16^2 **31** (A) 25^2-12^2 **769** (B)
483	3*7*23	22^2-1^2 **485** (B) 38^2-31^2 **2405** (B) 82^2-79^2 **12965** (B)	**485**	5*97	1^2+22^2 **483** (A) 14^2+17^2 **93** (B) 51^2-46^2 **4717** (B)
487	Primo		**489**	3*163	83^2-80^2 **13289** (B)
491	Primo		**493**	17*29	3^2+22^2 **475** (A) 13^2+18^2 **155** (A) 23^2-6^2 **565** (B)
495	3^2*5*11	24^2-9^2 **657** (B) 28^2-17^2 **1073** (B)	**497**	7*71	39^2-32^2 **2545** (B)

		$32^2–23^2$ **1553** (B) $52^2–47^2$ **4913** (B) $84^2–81^2$ **13617** (B)			
499	Primo		**501**	3*167	$85^2–82^2$ **13949** (B)

Bibliografía

[1] Sartorius von Waltershausen, Wolfgang. *Gauss zum Gedächtniss*. S. Hirzel, Leipzig, 1856. Reimpreso por Martin Sändig, Wiesbaden, 1965.

[2] Simmons, George F. *Calculus Gems*. Mathematical Association of America, 2007.

[3] Mackenzie, D. *Homage to an Itinerant Master*. Science 275:759, 1997.

[4] Zerger, Monte J. *A Quote a Day Educates*. Mathematical Intelligencer, vol. 20, no. 2, pp. 5-6, Spring 1998.

[5] Sautoy, Marcus du. La Música de los Números Primos. El enigma de un problema matemático abierto. Acantilado, 2007.

[6] Volovich, Igor V. *Number Theory as the Ultimate Physical Theory*. P-adic Numbers, Ultrametric Analysis and Applications, 2:1, 77-87, 2010. Disponible en Internet.

[7] Tegmark, Max. *Our Mathematical Universe. My Quest for the Ultimate Nature of Reality*. Alfred A. Knopf, 2014.

[8] Chaitin, Gregory. Los Límites de la Razón. Investigación y Ciencia, Mayo 2006, pp. 58-65.

[9] Dickson, L.E. *History of the Theory of Numbers*. Vol. 2. Chelsea Publishing Co., New York 1920.

[10] Hardy, G.H. & Wright, E.M. *An Introduction to the Theory of Numbers*, 5th ed. Clarendon Press, pp. 13 y 219, 1979.

[11] Conway, J.H. & Guy, R.K. *The Book of Numbers*. Springer-Verlag, pp. 146-147 y 220-223, 1996.

[12] Hardy, G.H. Apología de un matemático. Nivola, 1999.