Estudios Filosóficos LXXII (2023) 341 ~ 360

EN UN PRINCIPIO FUE EL NÚMERO

IN THE BEGINNING IT WAS THE NUMBER

Santiago Pérez-Cacho García
Universidad de Valladolid

La Matemática es la reina de las Ciencias y la Teoría de Números es la reina de la Matemática (Carl Friedrich Gauss)

Resumen: ***Dos anotaciones marginales, una de Fermat y otra de Riemann, han sido origen de dos de los principales problemas de la Teoría de Números, uno resuelto hace menos de treinta años, y otro aparentemente tan intratable como el anterior. Junto a conjeturas más fáciles de enunciar –Goldbach, Collatz, primos gemelos– pero aún sin resolver, la teoría de números, en un tiempo considerada sin utilidad, como proclamó Hardy, se ha revelado fundamental en criptografía.***

Palabras clave: ***Fermat, Riemann, Hardy, Criptografía.***

Abstract: ***Margin notes by Fermat and Riemann were the source of two key Number Theory problems. The former remained unresolved for over 300 years, until less than 30 years ago, and the latter is proving to be as intractable. Encompassing other easier to state but yet unresolved conjectures (such as Goldbach, Collatz, and twin primes), Number Theory, once deemed useless as Hardy claimed, is now considered fundamental to Cryptography.***

Keywords: ***Fermat, Riemann, Hardy, Cryptography.***

El número ¿se descubre o se crea? Es la pregunta que cabe hacerse de toda la matemática, y para el número la respuesta debe ser que el número se crea por necesidad. Diferentes culturas han creado los números y sus distintas representaciones –sistemas de numeración– motivadas por necesidades de cuantificar la magnitud discreta y de medir la continua. Por eso el número natural y el racional (fraccionario, es decir, cociente de dos naturales) surgen como logros matemáticos de importancia capital.

Es difícil situar el momento en que, en la temprana infancia, el niño "encuentra" el número y lo convierte, de una suerte de cantinela repetitiva, muy alejada de la que Antonio Machado recoge en su "Recuerdo infantil":

> *mil veces ciento, cien mil;*
> *mil veces mil, un millón.*

en un útil que lo acompañará toda su vida.

Una de las primeras propiedades que se aprecian tanto en el número natural como en el racional es el orden: dados dos números cualesquiera, a y b, o bien es a mayor que b, o a es menor que b o ambos son iguales. Sin embargo, existe una diferencia esencial entre el orden cuando se restringe a los naturales y el que se obtiene cuando se extiende a los racionales. En el primer caso, cada número posee un sucesor inmediato y, salvo el 0 –si lo incluimos como natural–, un predecesor, mientras que en los números racionales carece de sentido hablar del número inmediatamente anterior o posterior a un número dado, ya que entre cada dos números racionales existe otro (y, por tanto, una infinidad de ellos), lo que se expresa diciendo que el orden de los racionales es "denso". Jorge Luis Borges recrea este concepto de densidad de los racionales en su relato "El libro de arena", un libro en el que es imposible hallar la primera página – también la última – por mucho que nos aproximemos a la portada para abrirlo. Escribe Borges:

> Apoyé la mano izquierda sobre la portada y abrí con el dedo pulgar casi pegado al índice. Todo fue inútil: siempre se interponían varias hojas entre la portada y la mano. Era como si brotaran del libro.

La imagen del número 0 como portada del libro y cada página asociada a un racional nos explican el fenómeno: no hay ningún número racional sucesor inmediato del 0. Por muy próximo al 0 que elijamos un número, existe otro –de hecho, una infinidad– menor que él y por tanto más próximo al 0; son las hojas que parecen brotar del libro interponiéndose entre la portada y la *página* seleccionada.

El concepto de número es independiente del sistema que empleamos para representarlo; la numeración romana es un ejemplo claro, y todavía hoy seguimos utilizando para aplicaciones muy concretas –medida del tiempo,

coordenadas geográficas o astronómicas– el sistema de numeración sexagesimal, que tuvo su origen en Mesopotamia. Pero la elección del sistema tiene más importancia que el permitir escribir cada número, y ello se percibe en nuestro actual sistema de numeración, posicional y de base diez, que hace que cualquier número natural pueda escribirse utilizando tan solo símbolos elegidos entre un total de 10, los que llamamos dígitos: 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9 y, sobre todo, facilita operaciones tan básicas como suma, producto, resta y división al reducir el proceso a la memorización de las sumas o de los productos de cada par de dígitos; son las tablas de sumar y multiplicar que se aprenden en la escuela. Y de hecho nuestra operativa con números es, esencialmente, una operativa con números naturales, pues cuando operamos con racionales con una cantidad finita de cifras decimales solo al finalizar el cálculo ajustamos la coma decimal. El dominio de estos algoritmos de cálculo elemental permitió arrumbar el ábaco. La irrupción de las calculadoras, omnipresentes en dispositivos como los teléfonos móviles, ha modificado de manera esencial la situación.

La incorporación de los números enteros negativos supuso que se pudiera sumar, restar y multiplicar sin restricciones en este nuevo campo, estructura algebraica que se conoce con el nombre de "anillo"[1]. Sin embargo, no siempre es posible la división; refiriéndonos por ahora a los enteros positivos, existe la que se llama división euclídea: dados dos números naturales a y b, con a mayor o igual que $b \neq 0$, existen dos números naturales c y r, con r menor que c, tales que $a = b \times c + r$. Los números c y r son, respectivamente, el cociente y el resto de la división, y cuando el resto vale cero se dice que la división es exacta. En este caso, a se llama múltiplo de b o, equivalentemente, b divisor de a. La condición de ser un número divisor de otro es transitiva, pues si c es divisor de b y b es divisor de a, entonces c es divisor de a. Esta definición se extiende inmediatamente a los enteros. Para hacer posible siempre la división –excepto por 0– hay que extender el campo a los números racionales, obteniendo así una estructura más rica, la de cuerpo. La incorporación de los números irracionales, cuya existencia tuvieron que admitir los pitagóricos, completan lo que se llama la "recta real", en la que cada punto queda asociado de manera única con un número y recíprocamente. Se crea así un cuerpo, el de los números reales, base del análisis matemático. Pero aún quedaba una ampliación, la que desde el siglo XVI se venía manejando con cierto recelo pero que no se podía soslayar, y es la

[1] El conjunto de los números enteros, con las dos operaciones de suma y producto, constituye lo que se llama un anillo. La suma es asociativa, conmutativa, existe un elemento neutro, el 0, y cada número tiene un opuesto que sumado con él da 0. El producto es asociativo y conmutativo y ambas operaciones están ligadas por la propiedad distributiva: cualesquiera que sean los números enteros a, b y c, se cumple que $a(b+c) = ab+ac$. Por existir el número 1, elemento neutro para el producto, los enteros forman un anillo conmutativo (por serlo el producto) y unitario.

de los números complejos. Al resolver algunas ecuaciones de tercer grado, que tenían soluciones reales, aparecían raíces cuadradas de números negativos, lo que carecía de sentido, ya que el cuadrado de cualquier número real es siempre mayor o igual que cero. Bombelli optó por operar algebraicamente con estas expresiones[2] de la forma $a+b\sqrt{(-1)}$, y al final del cálculo resultaba que se cancelaban los términos en que aparecía $\sqrt{(-1)}$, dejando la solución real. Euler introdujo el símbolo *i* (por *imaginarium*) para representar al número $\sqrt{(-1)}$, y las expresiones $a+bi$ se incorporaron con el nombre de números complejos. Se podían sumar, restar, multiplicar y dividir –excepto por 0– y el resultado era de nuevo un complejo, con las mismas propiedades que definen un cuerpo como el de los números reales, que se podían identificar con los complejos de la forma $a + 0.i$. Pero los complejos ya no cabían en la recta real, y su morada resultó ser el plano, donde, fijados unos ejes de coordenadas, al complejo le correspondía el punto (a, b); a era la parte real y b la parte imaginaria. Pero se perdía lo que hasta entonces era una seña de identidad en los conjuntos numéricos que se habían ido incorporando: el orden. No en vano los números se crearon inicialmente para contar y medir, lo que supone comparar y ver si un número es mayor o menor que otro. La recta real hacía sensible la ordenación, y el problema era que no se podía encontrar sitio en la misma para acomodar a $i = \sqrt{(-1)}$. El propio Leibniz calificó al número *i* como un "anfibio entre el ser y el no ser", ni mayor que cero ni menor que cero. Al identificar a los complejos con los puntos del plano quedó clara su posición, y la ganancia que se consiguió fue infinitamente superior que la pérdida de la relación de orden entre ellos.

Un concepto importante, introducido por Gauss en su monumental obra *Disquisitiones Arithmeticae*, es el de congruencia. Fijado un número natural m, llamado módulo, dos números enteros a y b son congruentes módulo m cuando $a - b$ es múltiplo de m o, lo que es equivalente, si a y b dan el mismo resto al dividirlos por m, lo que se expresa de la siguiente manera:

$$a \equiv b \pmod{m} \text{ o bien } a \equiv b \ (m)$$

Este concepto permite clasificar los números enteros en clases, agrupando en cada una de ellas todos los números enteros que son congruentes entre sí, y obviamente existen m clases, puesto que hay m restos posibles: 0, 1, 2,… $m - 1$. Se puede hacer una aritmética, que se llama modular, y sumar y multiplicar con números (mod m). Por ejemplo, si se toma 12 como módulo, la suma de 9 + 5 es 2, y el resultado justifica que a esta aritmética de módulo 12 se la llame "aritmética del reloj", ya que, en efecto, 5 horas después de las 9 son

[2] La ecuación $x^3=30x+36$ tiene como solución $x = 6$. Si se aplica la fórmula que da las (posibles) soluciones, se llega a esta expresión: $x = (18 + \sqrt{-676})^{1/3} + (18 - \sqrt{-676})^{1/3}$. Nótese que, puesto que: $-676 = 26^2 . (-1)$, la expresión anterior se puede escribir así:

$$x = (18 + 26\sqrt{-1})^{1/3} + (18 - 26\sqrt{-1})^{1/3} = 3 + \sqrt{-1} + 3 - \sqrt{-1} = 6$$

Se han cancelado las raíces cuadradas de números negativos, obteniéndose la solución buscada. Este hecho se cumple siempre.

las 2: $5 + 9 \equiv 2 \pmod{12}$. Las reglas para operar son fáciles: cualquiera que sea el módulo m opérese con a y b en la forma usual, sumándolos o multiplicándolos, y luego tómese como resultado el resto de dividir por m el número obtenido en la operación. Así se asegura que dicho resultado sea uno de los m restos posibles, aunque podría tomarse igualmente cualquier otro número perteneciente a la clase, es decir, congruente con él. Este conjunto de restos módulo m es un anillo, si bien con un número finito de elementos.

La Teoría de Números

El número natural presenta, a pesar de su aparente simplicidad, una riqueza de matices que ha hecho que su estudio constituya una rama específica de la Matemática: la Teoría de Números. Una característica notable de la Teoría de Números que la hace más accesible para la divulgación es que su objeto de estudio es algo muy cercano, lejos de otros escenarios en los que la matemática se muestra mucho más hermética para el no matemático. A este respecto, y abundando en lo anterior, Harold M. Edwards, en un artículo publicado en 1978 afirma:

> En matemáticas. como en cualquier otro terreno, hay cuestiones no resueltas por doquier; para los matemáticos. la dificultad reside en dar con preguntas que puedan contestar y no al contrario. No es fácil, sin embargo, darle al lego ejemplos claros que ilustren este punto, porque el enunciado de las cuestiones de interés matemático suele requerir terminología especializada y formación suficiente. El teorema magno de Fermat es rara excepción a esta regla[3].

No obstante, existen ejemplos importantes en teoría de números que no requieren de conocimientos avanzados y que pueden comprenderse sin dificultad. Algunos de ellos son cuestiones abiertas, y las posibles líneas de ataque para resolverlas –en algunos casos, ni siquiera existen– son las que pueden requerir formación matemática específica para su comprensión.

Pero ¿qué es lo que hace a la teoría de números un campo singular dentro de la matemática? ¿Qué es lo que llevó a Gauss a calificarla como "Reina de la Matemática"? Posiblemente el hecho de que en ella se encuentre, como en ningún otro sitio, el espíritu que hace que su desarrollo solo busque la satisfacción del saber por el saber, sin ninguna intención utilitaria. Aquí procede recordar la frase de Jacobi, uno de los matemáticos preeminentes del siglo XIX: "La matemática existe por el honor del espíritu humano", y en su muy recomendable obra "Apología de un matemático", G.H. Hardy, uno de los matemáticos más eminentes de la primera mitad del siglo XX escribe:

[3] Harold M. Edwards, "El último teorema de Fermat", *Revista Investigación y Ciencia* 27 (1978), p. 44.

> Algunas veces se sugiere que la gloria de los matemáticos puros radica en la inutilidad de su trabajos y estos presumen de que no tengan aplicaciones prácticas. Esta imputación se basa habitualmente en un dicho osado atribuido a Gauss, según el cual, si las matemáticas son la reina de las ciencias, entonces la teoría de los números es, a causa de su suprema inutilidad, la reina de las matemáticas (nunca he sido capaz de encontrar la cita exacta)[4].

Pero el mismo Hardy añade más adelante que si la teoría de números se revelara como útil para lograr felicidad o alivio del sufrimiento humano ningún matemático rechazaría las posibles aplicaciones. Si se tiene en cuenta que el libro de Hardy se publicó por primera vez en 1940, cuando ya había estallado la segunda guerra mundial, se entiende su afirmación de que, dado que la ciencia sirve tanto para lo malo como para lo bueno, los matemáticos tengan motivo para "alegrarse de que haya una ciencia , y que sea la suya, cuya lejanía de las actividades cotidianas la mantiene apacible y limpia"[5].

El que originariamente la aparición del número buscara atender necesidades como las de contar y medir no puede ocultar el hecho de que se plantearan preguntas sobre el número en sí, alejadas de lo que serían cualesquiera otras condiciones derivadas de su uso.

Uno de los primeros descubrimientos relacionados con los números naturales fue el de número primo, el que no puede dividirse exactamente por otro, salvo por la unidad y por sí mismo. Y por contraposición, todos los restantes números se califican como compuestos, por poderse expresar como producto de otros números mayores que uno. El teorema fundamental de la aritmética afirma que todo número natural, o es primo, o se puede poner de manera única –salvo el orden– como producto de números primos. Enunciado así el teorema, es obligado considerar que el número 1 no es ni primo ni compuesto, ya que se podrían añadir como factores tantos 1 como se quisiera, perdiéndose la unicidad de la representación. Y puesto que existen infinitos números naturales, es obligado preguntarse si también será infinita la cantidad de números primos. La pregunta es claramente especulativa; obedece al espíritu de buscar el saber por el saber, sin que el resultado afirmativo o negativo vaya a aportar en principio ninguna utilidad.

La demostración de que, en efecto, existen infinitos números primos, se debe a Euclides, y merece la pena reproducirla aquí. Si solamente existiera un número finito de números primos, uno de ellos, p, sería el mayor de todos. Si ahora se forma el número $(2\times3\times5\times7\times11\times\ldots\times p)+1$ obtenido multiplicando todos los números primos hasta p y sumando 1 al resultado, es claro que ese número es mayor que p, por lo que no puede ser primo, ya que p era

[4] G.H. Hardy, *Apología de un matemático*", pp. 32-33. https://w3.esfm.ipn.mx/~cisneros/HardyApologiaEspanol.pdf

[5] *Ibid.,* p. 33.

el mayor de todos los primos. Por tanto, ese número ha de ser compuesto, y tendrá que ser divisible exactamente por algún primo, lo que no puede ocurrir ya que, al dividirlo por cualquiera de los primos existentes, la división da de resto 1. En consecuencia, hay que rechazar que haya un número finito de números primos.

La demostración anterior, elegante por su simplicidad, pone de manifiesto una de las características que surgen en la mayoría de los casos al tratar con números, y es la de intentar doblegar de alguna manera el infinito. Pero el infinito suele estar presente en muchas de las cuestiones que pueden plantearse relacionadas con los números naturales, y no siempre es posible vencerlo. Los siguientes son ejemplos que demuestran este hecho:

¿Existen infinitos primos gemelos, esto es, que se diferencien en dos unidades?

¿Existen infinitos primos de la forma n^2+1?

¿Existe siempre un número primo al menos entre n^2 y $(n+1)^2$?

Todo número par mayor que 2 ¿se puede poner como suma de dos primos?

Esta última cuestión es la conjetura de Goldbach, planteada en 1742. Las cuatro preguntas anteriores son desafíos de enunciado muy elemental, pero cuya resolución está pendiente. Y ello porque el número de casos que cada uno presenta es infinito.

Pero sería erróneo concluir que, cuando se está tratando con un problema planteado en un conjunto en el que las posibilidades son finitas, la solución es factible sin más que ir examin*á*ndolas una por una. En teoría, es posible, pero puede ser impracticable. *É*ste fue el procedimiento para demostrar el teorema de los cuatro colores, cuando las diferentes configuraciones que puede adoptar cualquier mapa plano se redujeron a un número finito, aunque grande, y se fueron analizando una por una hasta llegar el resultado de que es posible colorear cualquier mapa plano con sólo cuatro colores, de manera que regiones con una porción de frontera común reciban coloraciones distintas. La clave fue el uso del ordenador para el análisis de dichas configuraciones, pero si su *número hubiera sido*, por ejemplo, del orden de 10^{20}–un uno seguido de veinte ceros– el procedimiento hubiera sido imposible, aunque el ordenador examinara un millón de ellas cada segundo.

No hace falta alejarse mucho de los números naturales para encontrar situaciones en las que se buscan respuestas a una cuestión entre un número finito de posibilidades, e irlas examinando una por una no es la mejor estrategia para hallarlas. Concretamente, el descomponer un número que sea producto de dos números primos en sus dos factores es un problema difícil si el número es grande. Y sin embargo este es un problema en el que únicamente hay que explorar un número finito de casos, sin más que ir dividiendo el número por

los números primos a partir de 2 hasta obtener una división exacta, lo que seguramente ocurrirá antes de llegar, en el caso más desfavorable, hasta el número primo igual o inmediatamente menor que la raíz cuadrada del número a descomponer.

Si se quiere factorizar un número del orden de 1.000.000.000.000 tendríamos, para seguir al pie de la letra lo indicado, de disponer de los números primos menores que 1.000.000, que es del orden de la raíz cuadrada del número considerado, y de los que hay un total de 78498. Esto supone conocerlos de antemano o, si este no es el caso, ir calculándolos según se va avanzando para luego dividir por ellos, lo que consume tiempo de ordenador. Pero también se podría optar por ir dividiendo por todos los números a partir de 2, sin diferenciar si son o no primos; si el número que se busca factorizar no es divisible por 3, no lo será por 9, ni por 27, etc., pero puede que consuma menos tiempo esta manera de actuar, a pesar de que entonces ya no habría que realizar un máximo de 78498 divisiones, sino en el caso más desfavorable, del orden de 500.000, notando que se pueden dejar de lado, como divisores, los números pares si el número a descomponer es impar. De cualquier forma, y para el uso que se da a los números naturales en algunas aplicaciones que se verán posteriormente, el número 1.000.000.000.000 es pequeño. Lo normal es utilizar números de más de 200 cifras, y se han desarrollado algoritmos más eficientes que el de "fuerza bruta" antes descrito. Pero el problema de la factorización es difícil, muy difícil para números enormes, y contrasta con la facilidad que nos ofrecen los ordenadores para multiplicar dos números realmente grandes, que no es otra cosa que el proceso inverso al de factorizar.

La factorización de un número pone de manifiesto lo que se podría calificar como el ADN del número, y muchas de las propiedades de éste se pueden obtener de la misma. El siguiente ejemplo ilustra este hecho: uno de los problemas en los que la naturaleza de los factores primos de los números involucrados es decisiva se refiere a caracterizar los números naturales que pueden escribirse como suma de dos cuadrados. Lo sorprendente es que este problema, que tiene que ver con la adición, tenga su solución en aspectos multiplicativos. Si se comienza a buscar entre los números menores que 20, se encuentra que 1, 2, 4, 5, 8, 9, 10, 13, 16, 17 y 18 son, cada uno de ellos, suma de dos cuadrados, mientras que 3, 6, 7, 11, 12, 14, 15, y 19 no se pueden poner como suma de dos cuadrados. (Se ha incluido el número 0 como posible sumando, ya que $0 = 0^2$). En cada una de las dos listas aparecen números primos y compuestos, sin que se pueda adivinar un criterio para reconocer qué es lo que hace a un número ser suma de dos cuadrados y qué no se lo permite a otro. Ciertamente, la muestra considerada es muy pequeña, pero, aunque se amplíe hasta 40, se sigue sin ver que característica poseen estos números,

1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37 y 40

que los diferencia de estos otros,

3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, 28, 30, 31, 33, 35, 38 y 39.

Parece ser que fueron Albert Girard, y luego Fermat, los primeros en percibir la propiedad que caracteriza a los números de la primera lista, y si se ha traído aquí el problema es porque la razón de fondo se esconde en lo que antes hemos calificado de ADN de los números; en efecto, se halla en los factores primos de cada uno de ellos. La pista la da la siguiente identidad algebraica:

"Cualesquiera que sean los números a, b, c y d, se cumple que

$$(a^2+b^2)\,(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2.$$

Esto es: si un número es producto de dos cada uno de los cuales es suma de dos cuadrados, el número también es suma de dos cuadrados. De aquí que baste ceñirse, en principio, a considerar los números primos que son suma de dos cuadrados, puesto que los números que se obtengan como producto de ellos serán también suma de dos cuadrados. En la primera lista aparecen 2, 5, 13, 17, 29 y 37, y cada uno de ellos es suma de dos cuadrados, como se comprueba inmediatamente, mientras que ninguno de los primos de la segunda, 3, 7, 11, 19, 23 y 31 lo es. ¿Qué tienen en común los números primos de la primera lista? Pues que, excepto el 2, que es caso especial, todos ellos dan resto 1 al dividirlos por 4. En cambio, todos los primos de la segunda lista dan resto 3 al dividirlos por 4. Fermat afirmó, sin demostrarlo, que el número 2 y los números primos de la forma $4n + 1$ se pueden expresar de manera única como suma de dos cuadrados[6], lo que no ocurre para los primos de la forma $4n + 3$. Se ha establecido así, en el conjunto infinito de los números primos mayores que 2, una clasificación que depende del resto que da cada uno de ellos al dividirlo por 4: cada número primo es de la forma $4n + 1$ o $4n + 3$. Y de nuevo surge la pregunta: ¿alguna de estas clases contiene solamente un número finito de números o ambas son infinitas? La respuesta es que ambas son infinitas, siendo la demostración más directa la que se apoya en un resultado obtenido por el matemático alemán Dirichlet en 1837, que afirma que si los números a y b son primos entre sí (es decir, no tienen ningún divisor en común salvo el 1) entonces la progresión aritmética $\{an + b\} = \{a + b, 2a + b, 3a + b, 4a + b \ldots\}$ contiene un número infinito de números primos. Si se aplica este resultado con $a = 4$ y $b = 1$, se llega a que existen infinitos números primos de la forma $4n + 1$; para $a = 4$ y $b = 3$ el teorema asegura la existencia de infinitos primos de la forma $4n + 3$.

El resultado final es que los números que son sumas de dos cuadrados son aquellos cuyos factores primos son de la forma $4n + 1$, y si existen factores

[6] La demostración, un siglo después, se debe a Euler.

de la forma $4n + 3$ deben estar elevados a una potencia par. Por ejemplo, la descomposición en factores primos de 45 es $45 = 5x3^2$, y 45 es suma de dos cuadrados, 9 y 36, porque 5 es de la forma $4n + 1$ y 3, de la forma $4n + 3$, está elevado al cuadrado.

Desde muy antiguo existen creencias relacionadas con los números naturales que atribuyen a algunos unas cualidades místicas, y no podemos dejar de señalar que aún hoy hay muchas personas que consideran al número 13 como aciago, propiciando mala suerte. La disposición de números en algunos diseños planos, como los cuadrados mágicos –del que es exponente destacado el de Durero en su grabado "Melancolía I"– o el triángulo de Pascal, son prueba evidente del interés suscitado por los números en aspectos alejados del contar.

Los pitagóricos se ocuparon de los números llamados perfectos, que son aquellos que coinciden con la suma de sus divisores propios, es decir, los que prescinden del propio número como divisor. Los números perfectos no abundan mucho, por lo que su excelencia estaba asociada a su escasez; los tres primeros son 6, 28 y 496. La comprobación de que son perfectos es inmediata:

Número	**Divisores propios**	**Suma de divisores propios**
6	1, 2, 3	1+2+3 = 6
28	1, 2, 4, 7, 14	1+2+4+7+14 = 28
496	1, 2, 4, 8, 16, 31, 62, 124, 248	1+2+4+8+16+31+62+124+248 = 496

Y hay que remontarse a 8128 para obtener el siguiente. La pregunta que procede hacer es la siguiente: ¿existe un patrón que permita obtener números perfectos sin necesidad de hallar sus divisores propios? La respuesta es afirmativa: todo número de la forma

$$2^{n-1}(2^n - 1)$$

es un número perfecto si 2^n-1 es un número primo. Los tres casos que aparecen en la tabla, y el citado 8128, corresponden a n = 2, 3, 5 y 7; estos cuatro números perfectos se conocen desde Euclides, y al corresponder los valores de n a los cuatro primeros números primos constituye una tentación el suponer que para n = 11 el número 2^{11}-1 también será primo y dará origen a un nuevo número perfecto. Pero la hipótesis resulta falsa, ya que $2^{11}-1=2047=23\times89$ no es un número primo, y por tanto no da origen a un número perfecto.

Los números de la forma 2^n-1 se conocen con el nombre de "números de Mersenne", y es necesario que el exponente n sea un número primo para que el número 2^n-1 también sea primo, aunque el caso n = 11 muestra que no es

suficiente. Para n igual a 13, 17 y 19 se vuelven a obtener primos de Mersenne, pero para $n = 23$ el número resultante es compuesto.

¿Todos los números perfectos son de la forma anterior? La respuesta es que, si se buscan números perfectos pares, son necesariamente de esa forma. Por tanto, existirá un número infinito de números perfectos pares si existen infinitos números de Mersenne que sean primos, y ese es un problema abierto.

¿Existen números perfectos impares? No se conoce ninguno, aunque no se ha demostrado que no existan, pero se puede obtener una idea del tamaño que tendría un número tal en la sección "Juegos matemáticos" del número 172 de Investigación y Ciencia[7]. Hay que reconocer que los pitagóricos tuvieron clara la condición de excelencia que atribuyeron a los números perfectos dada su escasez.

Muy relacionados con los números perfectos son los números "amigos". El par más pequeño de números amigos es 220 y 284. Otros pares de números amigos son 1184 y 1210, o 2620 y 2924. La comprobación, con ayuda de un ordenador, es inmediata.

Existe una generalización de los números amigos, como es la que constituye una colección de números naturales de forma que la suma de divisores propios del primero sea igual al segundo, la del segundo sea igual al tercero, y así sucesivamente hasta que la suma de divisores propios del último sea igual al primero. He aquí una:

12496 ,14288, 15472, 14536, 14264.

Cuando se elige al azar un número natural, se calcula la suma de sus divisores propios, y se aplica al número así obtenido el mismo proceso, lo usual es que, finalmente, se llegue a un número primo, y en el paso siguiente se obtendrá 1. En el caso de obtener una serie de números que se repiten periódicamente como los antes citados, se ha encontrado un ciclo, y los números que se van repitiendo suelen describirse como la órbita del mismo. Los cinco números anteriores son los más pequeños que conforman un ciclo, y este hecho constituye una evidencia de la dificultad de encontrarlos por ensayo y error. Si se hubiera comenzado a explorar desde el 2 en adelante, primero se hubieran encontrado los números perfectos 6 y 28, que podrían describirse como ciclos de orden 1, y luego se encontrarían los números amigos 220 y 284, ciclos de orden 2, teniendo que esperar al número perfecto 496 para obtener otro ciclo de orden 1, seguidos de 1184 y 1210; solamente siete números hasta 1210, lo que indica su escasez.

Existe un concepto que se relaciona con los números perfectos y es el de "números perfectos en el sentido del indicador", que se definen a partir de la

[7] Ian Stewart, "Juegos matemáticos", en *Revista Investigación y Ciencia* 172 (1991), pp. 92 ss.

función "indicador de un número", $\phi(n)$, introducida por Euler, y que para cada número natural n devuelve el número de números primos con n menores que n. Por ejemplo, $\phi(15) = 8$, ya que hay ocho números primos con 15 menores que 15 : 1, 2, 4, 7, 8, 11, 13 y 14. Si se parte de un número cualquiera n, se calcula su indicador $\phi(n)$, y luego el indicador de este número, $\phi(\phi(n))$, y se continúa la iteración, los números sucesivos van siendo menores y al final se llega siempre a $\phi(2)$, que vale 1. En el caso de $n = 15$, estos son los resultados de la iteración:

$$\phi(15) = 8\ ,\ \phi(8) = 4\ ,\ \ \phi(4) = 2\ ,\ \ \phi(2) = 1.$$

Sumándolos todos se obtiene 8 + 4 + 2 + 1 =15, el número del que se partió. Se dice entonces que 15 es un número perfecto en el sentido del indicador[8].

Contrariamente a lo que ocurre con los números perfectos, estos nuevos números, que en la literatura matemática en inglés se conocen como "perfect totient numbers", resultado de la iteración del indicador –*totient* en inglés– son infinitos, ya que se puede demostrar fácilmente que todas las potencias de 3 son de esta clase. He aquí los primeros:

3, 9, 15, 27, 39, 81, 111, 183, 243, 255, 327,…

Se observa que todos ellos son múltiplos de 3, pero no es una característica que se cumpla siempre, aunque hay que llegar al número *4375 para encontrar uno que no es divisible por 3. Y por supuesto, todos son impares, ya que el indicador de un número distinto de 2 siempre es par, y los valores que se van obteniendo en las iteraciones sucesivas son pares salvo el último, que corresponde a* $\phi(2) = 1$.

La iteración usada en los ejemplos anteriores es un proceso común en matemáticas, y existe un problema no resuelto que depende de una iteración realmente simple. El proceso que da origen a esa iteración se basa en esta función, en la que n es un número natural:

$$f(n) = \begin{cases} \dfrac{n}{2} \text{ si } n \text{ es par} \\ 3n + 1 \text{ si } n \text{ es impar} \end{cases}$$

Si se comienza con $n = 12$, estos son los valores que se obtienen en las sucesivas iteraciones :6, 3, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1,… y se repite el ciclo 4, 2, 1. En caso de haber partido de 27, esta es la sucesión de iteradas: 82, 41, 124, 62, 31,.. y se recae en el mismo ciclo después de 111 pasos, llegando a números tan altos como 9232 antes de empezar a decaer.

[8] Laureano Perez Cacho, "Función suma de indicadores sucesivos", en *Revista Matemática Hispano Americana*, Madrid (1939) 45-50.

¿Ocurre siempre esto? Esta es la conjetura de Collatz[9], que fue el matemático que la enunció en los años treinta del siglo pasado. La evidencia computacional parecería garantizarlo, pero un número finito de casos no permite asegurar nada.

Todos los ejemplos anteriores constituyen problemas planteados, algunos resueltos y otros no, que no se pueden calificar como "matemática útil", lista para ser aplicada a situaciones en física, química, economía, sociología, astronomía, etc. Responden al deseo de saber por el saber, de intentar conquistarlas simplemente porque están ahí. El ejemplo que se recoge a continuación ha hecho historia, y merece un tratamiento más detallado.

La ecuación que es objeto del último teorema de Fermat es una ecuación diofántica, llamada así en honor de Diofanto de Alejandría, matemático del siglo III. Una ecuación diofántica es una ecuación con más de una incógnita, que por esa razón puede tener muchas soluciones, incluso infinitas, pero de la que solamente interesan las soluciones enteras –a veces limitadas a las naturales–. Fermat hizo su anotación marginal, en la que afirmó que la ecuación $x^n+y^n=z^n$ no tiene soluciones en números enteros positivos para n mayor que dos, en una página de la Aritmética de Diofanto, y añadió que disponía de una demostración realmente maravillosa, pero que el margen era demasiado estrecho para contenerla. Desde ese momento, el problema se convirtió en uno de los más famosos, si no el que más, de la teoría de números durante más de trescientos años. Fermat solo demostró que la ecuación anterior no tenía solución cuando n era igual a cuatro, caso previo a una demostración general en la que bastaría considerar los valores de n que fueran números primos. Para $n = 4$ utilizó un método, el "*descenso infinito*", basado en suponer que existe una solución en números naturales y a partir de ella deducir, por manipulación exclusivamente algebraica, otra solución con números naturales menores que la supuesta. Repitiendo el mismo método con esta nueva solución, se obtendría otra con números menores aún, pero este descenso no puede seguir indefinidamente pues por debajo de los números de la supuesta solución solo hay un número finito de posibles soluciones.

Euler demostró el caso $n = 3$, y posteriormente otros matemáticos fueron haciendo aportaciones y demostrando casos particulares, pero no se vislumbraba un método que pudiera tratar con todos los exponentes a la vez, única manera de demostrar el teorema. El comentario de Fermat, afirmando que había encontrado una demostración maravillosa, hacía pensar en la posibilidad de descubrir alguna identidad algebraica que permitiera atacar el problema. La primera mitad del siglo XIX vio como casos particulares del teorema de Fermat caían demostrados por diferentes matemáticos: en 1832, Dirichlet lo demostró para $n = 14$, y Lamé, en 1839, para $n = 7$. El caso $n = 5$ fue probado

[9] Patrick Honner, "Juegos matemáticos", en *Revista Investigación y Ciencia* 548 (2022) 63-66.

por Legendre en 1825, y el propio Gauss dio una demostración para el caso $n = 3$ distinta de la dada por Euler[10]. Pero el goteo de casos aislados evidenciaba la falta de una "magna idea" que pudiera aplicarse a todos los exponentes. Y en el año 1847, en una sesión de la Academia de París, dos matemáticos de renombre, Lamé y Cauchy, afirmaron por separado que estaban a punto de probar el teorema. Sin embargo, existía en sus demostraciones un fallo que fue comunicado en otra sesión académica cuando se hizo público un escrito remitido por un matemático alemán, Kummer, en el que señalaba el uso de un teorema de factorización única que, siendo cierto para los enteros, no lo era en algunos anillos construidos para abordar la demostración del teorema de Fermat. Kummer soslayó el problema y pudo llevar la demostración de golpe para incluir todos los exponentes primos hasta 100, salvo 37, 59 y 67, a los que calificó de primos irregulares. Era un avance importante, sin duda, pero el problema seguía allí, sin que se viera una línea de ataque que pudiera conducir al ansiado final.

La primera mitad del siglo XX vio cómo disminuía el interés por un tema que no era prometedor en cuanto a resultados. La obra de Ribenboim[11], publicada sólo quince años antes de que se consiguiera la demostración del teorema de Fermat, recoge la historia del mismo desde sus inicios, y en ella aparece la mención a curvas elípticas, que jugarían un papel decisivo en la demostración del teorema, con unos *método*s totalmente inimaginables en la época de Fermat. Todo se basa en la relación, formulada inicialmente como conjetura y en la actualidad demostrada como teorema, entre curvas elípticas y formas modulares que avanzaron en la década de los cincuenta del siglo XX dos matemáticos japoneses, Yutaka Taniyama y Goro Shimura.

Una curva elíptica, o cúbica elíptica, es una curva definida por una ecuación del tipo: $y^2 = x^3 + ax^2 + bx + c$, donde a, b y c son, en el caso que interesa para relacionarla con el teorema de Fermat, números enteros, con la restricción de que el polinomio $x^3 + ax^2 + bx + c$ no tenga dos raíces iguales.

Las formas modulares son más difíciles de describir: son funciones de variable compleja definidas en el semiplano superior del plano complejo –es decir, en los complejos $x + i\,y$ con $y > 0$[12]. Lo que interesa resaltar es que la conjetura de Taniyama y Shimura afirma que cada curva elíptica está asociada a una forma modular, lo que es suficiente para entender la argumentación

[10] Contrasta este hecho con el poco interés que mostró Gauss por el teorema de Fermat, como queda de manifiesto en la contestación a una carta que le fue enviada por su amigo, el astrónomo Olbers, en la que le indicaba que se había convocado un concurso por parte de la Academia Francesa de las Ciencias. Escribe Gauss: "Agradezco sus noticias relativas al premio de París. Pero confieso que el teorema de Fermat, como proposición aislada, tiene muy poco interés para mí, porque yo mismo podría plantear una multitud de cuestiones semejantes que no sería capaz ni de demostrar ni de refutar".

[11] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, New York, Springer, 1979.

[12] Y. Hellegouarc, "Fermat, demostrado al fin", en *Revista Investigación y Ciencia* 237 (1996) 60-65.

que llevó a la demostración del teorema de Fermat. Todo comenzó cuando Gerhard Frey, en un simposio que tuvo lugar en el año 1984, razonó suponiendo que el teorema de Fermat fuera falso, y que para algún $n > 2$ existieran enteros no nulos A, B y C tales que $A^n + B^n = C^n$. Pudo entonces construir la siguiente curva asociada a la hipotética solución de la ecuación de Fermat: $y^2 = x(x–A^n)(x+B^n)$. Esta es una curva elíptica –se la conoce con el nombre de curva de Frey– y no es modular por no poderla asociar con una forma modular por lo que, si la conjetura de Taniyama y Shimura es cierta, tal curva no puede existir. Pero tal curva se ha construido a partir de una hipotética solución de la ecuación de Fermat, por lo que negar la existencia de la curva es negar que la solución a la ecuación de Fermat exista: el teorema queda demostrado a expensas de demostrar la conjetura de Taniyama y Shimura y de probar que, en efecto, una curva de Frey no puede ser modular, lo que fue demostrado por Kenneth Ribet. En junio de 1993 Andrew Wiles, en unas conferencias que se celebraron en Cambridge, anunció que había demostrado el teorema de Fermat, pero en las revisiones encomendadas a varios equipos de matemáticos se encontró un paso que no estaba justificado. Después de siete años de trabajo en solitario, Wiles se encontraba en un atolladero. Optó por invitar a Richard Taylor a unirse a él y en octubre de 1994 se hicieron públicos dos artículos, uno firmado por Andrew Wiles y otro por Richard Taylor y Andrew Wiles que dejaban definitivamente cerrado el punto dudoso de la demostración. El teorema de Fermat dejaba de ser una cuestión abierta. La obra "El enigma de Fermat" de Simon Singh da cumplida cuenta de este final de la historia[13].

Inicio de la teoría analítica de números

La Teoría Analítica de números utiliza los recursos del análisis matemático para estudiar problemas relacionados con los números enteros. Es aparentemente paradójico el uso de una herramienta centrada en lo continuo para estudiar los números que se crearon para medir lo discreto. Pero la paradoja se difumina si se piensa que la mayoría de los resultados tienen un carácter global –por ejemplo, el teorema de los números primos, de naturaleza asintótica, es decir, cómo se comportan los números "en grande", al crecer ilimitadamente la cantidad de los mismos– en contraposición con el carácter local de la continuidad de una función, por citar lo más patente.

¿Cómo se presentan los números primos en la sucesión de números naturales? No hay pautas que predigan cuándo el sucesor de un número par va a ser un número primo. Hay primos separados tan solo por un número entre ellos –son los que se llaman primos gemelos– tales como 5 y 7, 11 y 13, o 17

[13] S. Singh, *El enigma de Fermat*, Barcelona, Planeta, 1998.

y 19, e intervalos donde todos los números son compuestos. Y de hecho se puede demostrar que existen intervalos tan grandes como se quiera en los que no hay ningún número primo, aplicando un razonamiento muy semejante al usado para probar que existen infinitos números primos[14]. Sin embargo, al considerarlos globalmente, se encuentran regularidades en la distribución. Gauss conjeturó que $\pi(x)$[15], función que da el número de primos menores o iguales que x, donde x es un número real, viene dado aproximadamente por el cociente entre x y el logaritmo natural de x:

$$\pi(x) \approx \frac{x}{\ln(x)}$$

(el símbolo $\approx$ se utiliza en el sentido de "aproximadamente igual que")

Una aproximación aún mejor es la dada por la siguiente integral, llamada Logaritmo integral y denotada $Li(x)$:

$$\pi(x) \approx Li(x) = \int_2^x \frac{dt}{\ln(t)}$$

La tabla adjunta ilustra cómo se comportan las tres funciones anteriores.

Número x	$\int_2^x \frac{dt}{\ln(t)}$	$\pi(x)$	$\frac{x}{\ln(x)}$
10000	1245	1229	1085
100000	9628	9592	8685
1000000	78626	78498	72382
10000000	664917	664579	620420
100000000	5762208	5761455	5428681
1000000000	50849233	50847534	48254942

(Se han redondeado los números de las columnas segunda y cuarta, ya que las dos funciones que aparecen encabezándolas no dan valores enteros).

Tal como se puede comprobar, en este rango de números, es mejor la aproximación que proporciona el logaritmo integral que la dada inicialmente por Gauss. En cualquier caso, y aunque los errores absolutos van creciendo,

[14] Un intervalo de 10000 números consecutivos en el que no hay ningún primo es el siguiente: si $n = 10001!$ (esto es, el producto de todos los naturales desde 1 hasta 10001), entonces todos los números $n + 2$, $n + 3$, $n + 4$,…, $n + 10001$ son compuestos, pues el primero es divisible por 2, el segundo lo es por 3, etc.

[15] En esta notación que es universal para representar el número de primos menores o iguales que x, el símbolo π *no tiene relación con el número "pi"*.

los errores relativos van disminuyendo, como demostraron en 1896., independientemente uno del otro, Jacques Hadamard y C. J. de la Vallée Poussin al probar que

$$\lim_{x\to\infty} \frac{\pi(x)\ln(x)}{x} = 1$$

Este resultado es el que se conoce como teorema de los números primos.

Treinta y siete años antes, en un trabajo de tan solo ocho páginas publicado en 1859, Riemann, uno de los grandes matemáticos del siglo XIX, aborda el problema de determinar el término que da el error que se comete al tomar como número de primos menores o iguales que x el valor del logaritmo integral. Busca, pues, hallar el número exacto de números primos menores o iguales que x, y no una aproximación asintótica como la del logaritmo integral o la de Gauss. Y lo logra haciendo uso de una función, ζ(s) –que a partir de ese momento se conocerá como la función zeta de Riemann– introducida por Euler[16] un siglo antes.

Para ello empieza por considerar la variable s, que en la serie de Euler es real, como compleja: $s=\sigma+i\tau$, y a continuación extiende la definición de la función a todo el plano complejo, salvo el punto $s = 1$ en el que la función toma un valor infinito. Luego demuestra que la función ζ(s) se anula en los números enteros negativos –2, –4, –6,…, llamados "ceros triviales", y en otra infinidad de puntos del plano, todos ellos localizados en una banda de anchura 1, $0 < \sigma < 1$, que también son "ceros" de la función, y son simétricos respecto del eje real – si $\zeta(\sigma+i\beta)=0$ también $\zeta(\sigma+i\beta)=0$ –. Tras calcular algunos, conjetura que todos ellos tienen su parte real igual a ½, es decir, se hallan sobre la recta $\sigma = ½$ y deja la siguiente frase, que por sus efectos en la matemática posterior se asemeja a la acotación hecha por Fermat en el margen de una página del libro de Diofanto: "Sería deseable, en todo caso, una prueba rigurosa de esto; mas yo, tras algunos breves intentos en vano, he dejado a un lado su búsqueda provisionalmente, dado que parecía superflua para el objetivo inmediato de mi investigación"[17].

La culminación del trabajo es una expresión, complicada, que da el número de números primos menores que un número x, y en la que uno de los

[16] $\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s}$ donde s es una variable real. La anterior suma infinita es lo que se conoce como serie, y en este caso converge, es decir, toma un valor finito, solo si $s > 1$. Euler obtiene la siguiente expresión:

$$\sum_{n=0}^{\infty} \frac{1}{n^s} = \frac{1}{1-\frac{1}{2^s}} \times \frac{1}{1-\frac{1}{3^s}} \times \frac{1}{1-\frac{1}{5^s}} \times \frac{1}{1-\frac{1}{7^s}} \times \frac{1}{1-\frac{1}{11^s}} \dots$$

que establece una relación entre todos los números naturales y los números primos.

[17] B. Riemann, "Sobre el número de primos menores que una cantidad dada", en B. Riemann, *Riemanniana selecta*, edición y estudio introductorio de José Ferreirós, Madrid, CSIC, 2000.

términos que aparecen es una serie[18] extendida a todos los ceros que se hallan en la banda crítica $0 < \sigma < 1$, lo que explica el interés por los puntos en los que $\zeta(s)=0$[19].

La hipótesis de Riemann se erige ahora como uno de los mayores retos matemáticos. Ya en el congreso de París de 1900 Hilbert la colocó entre los 23 problemas que deberían ser objeto de estudio en el siglo que comenzaba.

Los temas abordados hasta aquí lo han sido porque sirven, en principio, como ejemplos de la idea que Hardy mantiene en su obra "Apología de un matemático", al afirmar que las matemáticas «auténticas» de los «auténticos» matemáticos, es decir, las matemáticas de Fermat, o Euler, o Gauss, o Abel o Riemann, son totalmente «inútiles». Si Hardy se refería únicamente a las aportaciones hechas a la teoría de números por los matemáticos anteriormente citados, calificando esas matemáticas como inútiles, se le podría conceder algo de razón, pero el devenir del tiempo demostraría que en esto se equivocaba, como veremos posteriormente. En el trasfondo se encuentra la distinción, que luego matiza, entre matemática pura y matemática aplicada. Y se percibe un decantarse hacia el pacifismo al hablar de matemática "inocua", en un sentido claro al contraponerla con la química, por ejemplo, que no puede calificarse de igual modo ¿Qué aplicación puede tener el llegar a demostrar que existen infinitos primos de la forma $n^2 + 1$? ¿O el conocer que todas las trayectorias en el proceso iterativo de Collatz finalizan en la órbita 4, 2, 1? Y la demostración del teorema de Fermat ¿qué utilidad ha aportado? Ciertamente los tres ejemplos anteriores ilustran realidades matemáticas cuya utilidad fuera del campo de la matemática dista mucho de ser obvia.

Pero sostener que las matemáticas de Fermat, o Euler, o Gauss, o Abel o Riemann, son totalmente «inútiles» no puede aplicarse sin más al total de la obra matemática de los citados, pues, por ejemplo, Euler estudia la forma óptima de los cascos de los buques utilizando matemáticas, y Gauss apoya a los astrónomos que primero hallaron, y luego perdieron a Ceres, calculando los elementos de su órbita a partir de un número realmente escaso de observaciones, lo que permitió hallarlo de nuevo; esto por no citar sus contribuciones a la geodesia derivadas de su estudio teórico de las superficies. De cualquier forma, su obra "Disquisitiones Arithmeticae" lo sitúan en uno de los primeros puestos en el desarrollo de la teoría de números.

En la fecha en que se escribió la cita de Hardy, año 1940, la guerra mundial demandaba comunicaciones seguras para cada bando, e interceptación y descifrado de las mismas por parte del contrario, lo que se tradujo en un

[18] $\sum_\rho Li(x^\rho)$, donde recorre el conjunto de los ceros no triviales de la función ζ.

[19] Una descripción detallada de todo el proceso se encuentra en la obra John Derbyshire, *Prime Obsession. Bernhard Riemann and the greatest unsolved problem in mathematics,* New York, Plume, 2004.

crecimiento de la criptografía, conjunto de técnicas muy antiguas y diversas que comenzaba a estructurarse como ciencia. El reclutamiento de expertos en Gran Bretaña en los primeros meses del conflicto, y su acomodo en Bletchey Park, confirmó la tendencia que empezaba a surgir de ir aumentando el número de matemáticos para abordar el problema de romper el código alemán que utilizaba la máquina "Enigma".

Pero lo que colocó a la teoría de números en el centro de la criptografía moderna fue el desarrollo de internet, por la necesidad de hacer seguras las comunicaciones, sobre todo si implicaban transacciones de dinero. Había que crear claves para que los mensajes no los pudieran leer salvo los destinatarios. En una primera aproximación, si se ha de convenir una clave entre dos personas para poder comunicarse con seguridad, o tienen que reunirse para acordar dicha clave o han de confiar en un medio de transmisión (correo, teléfono) para hacerlo. Pero puede ocurrir que sea interceptado el mensaje sin que ellos sean conscientes y que la clave ya no sea segura ¿Se puede arbitrar un medio para conseguir acordar una clave dando a cada participante en la comunicación suficientes datos para obtenerla pero imposibilitando al posible interceptor de conocerla? La respuesta es afirmativa, y la solución la dieron Diffie y Hellman en 1976, causando un auténtico revuelo.

Cuando se examina el método seguido se comprueba que la matemática que se usa no es en absoluto complicada; se basa en crear "funciones trampa" de la forma $m= a^x \ (mod\ p)$[20]. Se llaman así porque es fácil calcular m conocidos a, x y p, pero prácticamente imposible calcular x conocidos m, a y p si p es suficientemente grande. Los ordenadores han facilitado el recorrido en sentido directo para construir la función trampa. No hay problema en elegir a, que usualmente se toma igual a 3 o a 5, y hay que utilizar el ordenador para elegir un número primo p muy grande, Una vez hecho esto, el cálculo de $m = a^x \ (mod\ p)$, que, recordemos es el resto de dividir a^x por p es casi inmediato aun para un x grande. Pero en sentido inverso, calcular x a partir de m, ya es otra historia.

El método de Diffie y Hellman no sirve para aplicaciones que requieran comunicaciones seguras entre muchos, como sucede cuando los clientes quieren acceder a un comercio para comprar on-line. La solución la dieron poco tiempo después tres matemáticos, Rivest, Shamir y Adleman, creando el método RSA ampliamente utilizado. Cada usuario tiene dos claves, una pública, que debe difundirla para que quien quiera comunicarse con él pueda hacerlo

[20] X e Y acuerdan los valores de a y p. X elige un número x, e Y elige y que se mantienen en secreto. X calcula $A = a^x \ (mod\ p)$, y se lo envía a Y. Y calcula $B= a^y \ (mod\ p)$ y se lo envía a X. Y puede calcular ahora $A^y = (a^x)^y \ (mod\ p)$ que es igual a $B^x = (a^y)^x \ (mod\ p)$. Este número es la clave. La única posibilidad de capturarla es cuando se envían por una línea de comunicación no segura los números A y B, pues se podrían calcular x e y, pero si, por ejemplo, $a = 3$ y p es un primo de más de 50 cifras, resulta prácticamente imposible.

utilizándola, y otra privada que debe guardar celosamente. El comercio, al igual que cualquier posible cliente, tiene también sus dos claves, la pública que deben conocer los clientes para comunicarse con él, y la privada que solo conoce él. Las claves, tanto la pública como la privada, son dos números muy grandes, y la clave privada es el producto de dos números primos de unas 200 cifras cada uno. El mensaje que se quiere mandar se codifica con la clave pública del receptor, y solamente éste podrá leerlo usando su clave privada para descifrarlo. La seguridad depende de la dificultad para factorizar la clave privada.

Treinta años después de la muerte de Hardy, la criptografía de clave pública desmintió la inutilidad de la teoría de números y la situó en una posición preeminente dentro del campo de la matemática aplicada. La evidencia que se impone es que la matemática siempre es potencialmente aplicable, y la tenida como la más pura e inútil se revela, cuando la ocasión surge, como una herramienta indispensable.

Los distintos desarrollos de la criptografía han incorporado otras técnicas para conseguir mayor seguridad en las comunicaciones y transacciones a través de internet[21]. Junto a necesidad de encriptados más difíciles de romper, se han ido produciendo ataques, muchas veces con fines delictivos, encaminados a descubrir fallos en los sistemas de encriptación, aunque en otras ocasiones el objetivo del atacante solo sea la satisfacción de superar el reto que supone vencer una dificultad "que está ahí". ¿No es éste un ejemplo más del saber por el saber que impregna a la matemática? Encontrar fallos y corregirlos es dar mayor seguridad a los usuarios.

Santiago Pérez-Cacho García
Departamento de Álgebra, Análisis Matemático, Geometría y Topología
Universidad de Valladolid
Paseo de Belén, 7, 47011
Valladolid
acadspc@uva.es

[21] Existe un método de criptografía utilizando curvas elípticas, y en una ambivalencia curiosa, hay un método de factorización, también usando curvas elípticas –que va por tanto en contra de la seguridad del sistema RSA al favorecer la descomposición del número clave en sus dos factores– desarrollado por el matemático Hendrik Lenstra.