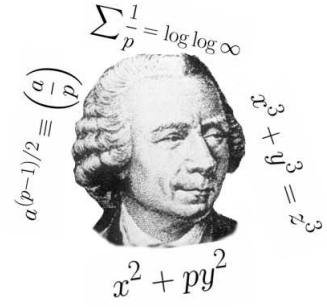
EULER Y LA TEORÍA DE NÚMEROS

FERNANDO CHAMIZO LORENTE



NOTA PRELIMINAR DEL AUTOR. Este artículo es una versión extendida de la charla que impartí en la Jornada Euler el 14 de febrero de 2007 en la Facultat de Matemàtiques i Estadística de la Universitat Politècnica de Catalunya. Agradezco a los organizadores la invitación así como el permiso para difundir este artículo.

Incluso limitándose a la contribución de Euler a la teoría de números fue necesaria una selección para ajustarse al tiempo fijado. Mi decisión fue evitar algunos temas que podrían ser tratados por otros ponentes, especialmente la combinatoria y el estudio de las funciones elípticas (que en tiempos de Euler no tenía el valor aritmético actual). Reconociendo lo arbitrario de la selección, he preferido conservarla aquí para ser fiel al material original.

Un último *caveat* es que de ningún modo soy un especialista en historia de las matemáticas y que las aserciones originales que pueda verter en este aspecto deben entenderse como meras opiniones. Me sentiría satisfecho si consiguiera divulgar con acierto una pequeña pero fundamental parte de la teoría de números en la que trabajó este gran genio de las matemáticas, LEONHARD EULER, cuyo tricentenario cumpleaños celebramos ahora.

1. En el siglo XVIII

Por mero instinto de superviviencia hay una tendencia entre los especialistas a sobredimensionar su propia disciplina, y no es raro que vaya desde el orgullo legítimo o el proselitismo militante a la depredación

despiadada o la crítica agresiva de lo ajeno. Es por ello que cuando examinamos las aportaciones de alguien al que se ajusta tan bien el neologismo "multidisciplinar", es fácil caer en la tentación de convertirle en uno de los nuestros. Las contribuciones de Euler en teoría de números son espectaculares pero sería una afirmación injustificable decir que ésta era el objeto de su principal interés. Es muy reveladora la frase de H.M. Edwards [Ed]:

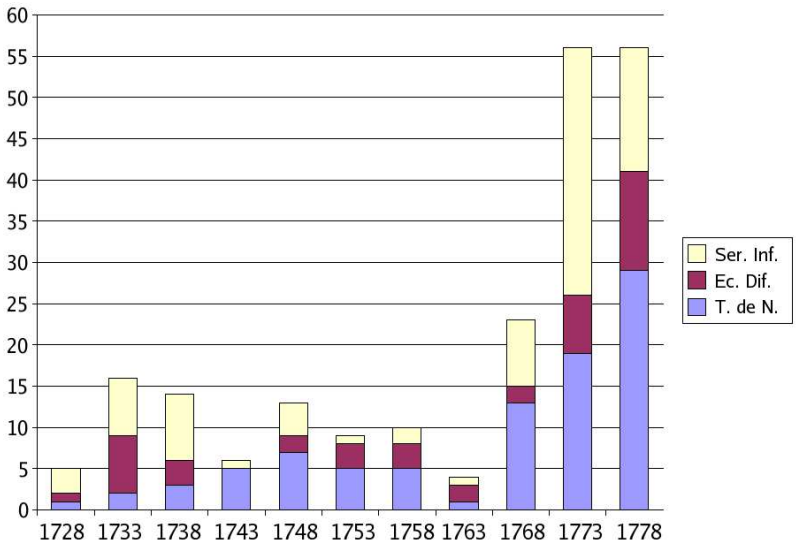
> Una medida de la grandeza de Euler es que cuando uno estudia teoría de números tiene la impresión de que Euler estaba principalmente interesado en teoría de números pero cuando estudia series divergentes siente que las las series divergentes eran su mayor interés, cuando estudia ecuaciones diferenciales uno imagina que realmente las ecuaciones diferenciales eran su materia favorita, y así sucesivamente...

Si queremos contrastar esta afirmación de forma tangible podemos tratar de contar el número de artículos dedicados por Euler a cada una de estas áreas como muestra de la porción del valioso tiempo que quiso ocupar con ellas a lo largo de su vida. Por supuesto hay varios errores de bulto en este intento, el mayor de ellos el que criticamos en muchas evaluaciones académicas: no es lo mismo contar que leer; también es difícil dividir exhaustivamente la obra de Euler en áreas por las continuas interrelaciones entre ellas. Para no contagiar este burdo recuento con los propios prejuicios tomemos como referencia la división de [Da] y sustituyamos el término "series divergentes" por "series infinitas", entonces el gráfico que obtenemos es el del principio de la página siguiente.

No hay una conclusión clara que se pueda extraer más allá del hecho de que su interés por la teoría de números fue constante a lo largo de su vida, aunque no fue cronológicamente su primer amor (de acuerdo con [We] el detonante fue la primera carta de C. Goldbach en 1729 y su insistencia posterior).

Parece pertinente entonces buscar entre los escritos de Euler una frase elogiosa y lapidaria, como la famosa de C.F. Gauss[1], para que los teóricos de números podamos justificar nuestras diversiones y adornar los libros. Pero antes al contrario, los elogios son un poco tibios. Así dedica

[1]"Las matemáticas son la reina de las ciencias y la aritmética la reina de las matemáticas".



la introducción de [E134] a justificar la investigación en teoría de números, y después de señalar que contiene "las verdades más recónditas" leemos:

> Por tanto, incluso si una proposición ya sea cierta o falsa parece que no redunda en ninguna utilidad para nosotros, todavía el método mismo por el cual se establece la certeza o falsedad usualmente abre el camino para que entendamos otras verdades más útiles. Por esta razón, creo firmemente que no he desperdiciado mi trabajo y mi esfuerzo en investigar estas propiedades que contienen notables propiedades sobre los divisores de los números. Esta teoría de los divisores no es de uso vano sino que alguna vez podría mostrar alguna utilidad no despreciable en análisis[2].

Por otro lado, Euler dedica la segunda parte de sus *Elementos de Álgebra* [EuAl] a la teoría de números y en la introducción escribe:

> Cuando el número de ecuaciones no se ajusta al de incógnitas [...] la materia es una rama particular del álgebra llamada *análisis indeterminado*.

[2]Véase [We] p.121–122 para una realización de esta utilidad según Euler.

> [...] usualmente se añade la condición de que los números buscados sean enteros y positivos, o al menos racionales [...]. Ocurre que esta parte del análisis frecuentemente requiere artificios ajustados a ella, los cuales hacen un gran servicio ejercitando el juicio de los principiantes y dándoles destreza en los cálculos.

¿Debemos pensar que para Euler la teoría de números era sólo un ejercicio para abrir la mente de los principiantes? ¿un entretenimiento calculístico? ¿una esperanza de aplicabilidad en otras áreas? ¿una disciplina subsidiaria del álgebra básica en su sentido originario de resolución de ecuaciones? Es difícil mantener que la entendiese como algo subordinado y tangencial teniendo en cuenta el hecho, no muy conocido, de que escribió una monografía inconclusa sobre el tema [E792].

Quizá la explicación está en la propia genealogía de la teoría de números: muchas veces se atribuye a P. Fermat la sistematización de esta área [To] o se dice que las *Disquisitiones Arithmeticae* [Ga] de 1801 son como los *Elementos* de Euclides para la geometría (no está de más señalar que tres libros de los *Elementos* ya se dedicaban a la aritmética). En la Europa de la Ilustración no había una gran tradición en teoría de números[3] que por otra parte estaba alejada de las ideas pragmáticas imperantes entonces (nótese la insistencia en la utilidad en las citas anteriores), según Euler [E134]:

> No faltan entre los grandes matemáticos quienes juzgan las verdades de este tipo como completamente estériles y por tanto indignas para afanarse en su investigación.

Por cierto, en contra de lo que normalmente se admite la denominación *teoría de números* ya aparece (quizá por primera vez) en uno de los trabajos de Euler [E279]. Para completar el contexto, nótese que, como señala A. Weil [We], los primeros matemáticos profesionales comenzaban a aparecer entonces.

---

[3]Según [Du] "Los matemáticos estaban entusiasmados por el poder del cálculo y su amplio campo de aplicaciones. En lenguaje moderno se diría que este tema estaba *caliente*. Por comparación la teoría de números apenas se consideraba un objeto matemático serio". También en [Sa] (Diciembre 2005) leemos "[Euler] escribió 96 [*sic*] artículos en el área y es una medida de la relativa baja estima en la que estaba la teoría de números que la mitad de esos trabajos se publicaron póstumamente".

La herencia de Fermat es patente en Euler de la misma forma que Gauss heredó problemas de Euler. Por completar la genealogía aritmética colindante con los tiempos de Euler hay que añadir los nombres de J.-L. Lagrange y A.-M. Legendre.


Fermat
(1601-1665)


Euler
(1707-1783)


Gauss
(1777-1855)


Lagrange
(1736-1813)


Legendre
(1752-1833)

Podríamos continuar esta tabla hacia adelante hasta nuestros días con innumerables ramificaciones, pero hacia atrás no hay tanto que decir. Por supuesto dos excepciones notables son los trabajos recopilados por Euclides y los grandes logros de la matemática hindú en la ecuación de Pell. Esta situación relativiza también el comentario de C. Truesdell en la introducción, siempre muy laudatoria, a [EuAl]:

> [Euler] recreó la teoría aritmética de números [. . .] Él dio a esta materia una nueva vida y descubrió en ella mayor número de grandes teoremas que todos los matemáticos anteriores juntos.

Más apropiada parece la frase de Edwards citada en [Du]:

> Sólo sus contribuciones a la teoría de los números serían suficientes para establecer una reputación duradera en los anales de las matemáticas.

Es instructivo analizar lo que puede encontrar el lector actual cuando compara a Euler con su antecesor Fermat y su sucesor Gauss. En la

comparación no hay mucho que decir sobre Fermat, ciertamente es genial y con seguridad utilizó con maestría su método del descenso y otras técnicas originales para probar muchas de sus afirmaciones, pero no hay una gran obra donde compilase sus resultados, conocemos muchas de sus investigaciones aritméticas a través de su correspondencia y ni siquiera hay demostraciones que leer (según se dice, sólo se conserva una), tampoco había revistas Matemáticas donde publicarlas. Gauss, por su parte, es completamente satisfactorio para el lector actual, los enunciados en [Ga] son claros y las demostraciones sintéticas e irrepochables, es notable que una obra juvenil sea tan madura, es como si hubiera estado pensando en ella durante toda una vida. Euler es muy diferente, visita recurrentemente los temas sin completarlos, las demostraciones a veces tienen puntos oscuros con respecto al rigor, experimenta con los números, parece como si a menudo escribiera a vuela pluma, tal como salen los temas de su mente (lo cual no es ilógico habida cuenta de su extensa obra). Hay un aspecto positivo en ello desde el punto de vista didáctico y es que es más fácil de entender la manera de razonar de Euler, sus intentos y descuidos nos acercan a la comprensión de la mente del genio mientras que Gauss se muestra impenetrable porque sólo vemos el producto en su fase final, las múltiples demostraciones de la ley de reciprocidad cuadrática no manifiestan diferentes estados, son completas por sí mismas (véase la opinión de Yu. Manin [Le]). Por otro lado, la forma de proceder de Euler ha dado lugar a una herencia matemática más generosa, abundantísima. Posiblemente nunca sepamos de cuántas matemáticas interesantes privó a las siguientes generaciones el lema "pauca sed matura" (poco pero maduro) de Gauss, mientras que Euler ofrece generosamente sus resultados y conjeturas para beneficio inmediato de todos, incluido Gauss que en [Ga] hace múltiples referencias a Euler.

2. Divisibilidad

Fue Goldbach quien parece haber despertado el interés de Euler en teoría de números al trasladarle la conjetura de Fermat acerca de la primalidad de los números $F_n = 2^{2^n} + 1$. De manera natural esto lleva a considerar la divisibilidad de potencias lo cual condujo a Euler a redescubrir el *pequeño teorema de Fermat* y dar su primera prueba conocida. Euler publicó tres pruebas de este resultado a lo largo de su

vida, [E54], [E134] y [E271] ([Su] indica cuatro) pero las dos primeras tienen sólo diferencias formales y Gauss parece reconocer sólo dos[4] en [Ga]. Volviendo a la comparación entre ambos genios, nótese que [E54] en el facsímile en [Da] se extiende a lo largo de seis páginas en cuarto, excesivo para los ojos actuales, mientras que en la traducción de [Ga] Gauss resume la demostración en apenas seis líneas.

La tercera demostración [E271] es la que parece satisfacer más a Euler (véase también el comentario de Gauss en la nota anterior) y le permitió una generalización bien conocida que basa el actual criptosistema RSA:

Congruencia de Euler-Fermat
Sea $\phi(n) = \#\{1 \leq m \leq n \ : \ \mathrm{mcd}(m,n) = 1\}$, *entonces para* a *y* n *coprimos se cumple* $a^{\phi(n)} \equiv 1 \pmod{n}$.

La demostración de la congruencia de Euler-Fermat hoy en día se reduce a notar que el orden de cualquier elemento del grupo multiplicativo $\mathbb{Z}_n^*$ debe dividir al orden del grupo, que es $\phi(n)$. Por supuesto, Euler no podía apelar a este resultado pero en cierta forma su demostración se basa en la idea de la partición en cogrupos [Su], [Di].

El pequeño teorema de Fermat es el caso $n = p$ primo, es decir $p|a^{p-1}-1$ si $p \nmid a$. Incluso este humilde resultado lleva a interesantes preguntas. Euler ya se percató de que era inusual que un número compuesto n verificase $n|a^{n-1} - 1$. Sin embargo existen algunos n llamados *números de Carmichael*, como $n = 561$, que satisfacen $n|a^{n-1} - 1$ siempre que a y n sean coprimos. Se conjeturó que sólo existía un número finito de ellos pero en 1994 W.R. Alford, A. Granville y C. Pomerance [AGP] sorprendieron a la comunidad matemática probando no sólo que hay infinitos sino que no están muy dispersos (el espaciamiento está acotado por una potencia no muy grande) lo cual choca con los experimentos numéricos.

A través del estudio de la divisibilidad de potencias, Euler pudo refutar la conjetura de Fermat probando explícitamente que F_5 no es primo porque $2^{2^5} + 1 = 641 \cdot 6700417$. A pesar de que el resultado ya aparece en [E54], no encontramos la explicación hasta [E134] (prueba que los

[4]En el Art. 50 menciona: "Como el desarrollo de una potencia binomial parecía bastante ajena a la teoría de números, Euler dio otra demostración".

factores deben ser de la forma $64n + 1$ [Su]). En artículos posteriores continuó su interés por el problema numérico de la factorización y generación de primos grandes (e.g. [E283], [E369]). El progreso de las computadoras y los algoritmos de primalidad nos permite conocer en la actualidad que $F_n = 2^{2^n} + 1$ es compuesto para $5 \leq n \leq 32$ y se conocen otros valores de n no consecutivos para los cuales también F_n es compuesto. De hecho no se ha encontrado ningún $n \geq 5$ tal que F_n sea primo. ¡La conjetura de Fermat fue muy arriesgada!

Euclides de Alejandría

Otro de los temas relacionados con la divisibilidad que trató Euler fueron los *números amigos* y los *números perfectos*. La investigación de los segundos parece comenzar en [E798]. Recordemos que un número N es *perfecto* si la suma de todos sus divisores es $2N$. Los dos primeros números perfectos son 6 y 28:

$$12 = 1 + 2 + 3 + 6$$
$$56 = 1 + 2 + 4 + 7 + 14 + 28$$

Euclides había probado en el Libro IX de sus *Elementos* que si $2^{n+1} - 1$ es primo entonces $2^n(2^{n+1} - 1)$ es perfecto. La contribución de Euler fue probar, unos 2000 años después, que el recíproco se cumple para los pares, es decir:

Un número par N es perfecto si y sólo si $N = 2^n(2^{n+1} - 1)$ con $2^{n+1} - 1$ primo.

Una de las propiedades fundamentales notada por Euler sobre la función que asigna a N la suma de sus divisores, en notación moderna $\sigma(N)$, es la multiplicatividad [Sa]. Es decir, si n y m son coprimos $\sigma(mn) = \sigma(m)\sigma(n)$. Con ella no es difícil probar que si N es perfecto y par, digamos $N = 2^n m$ con $2 \nmid m$, entonces debe cumplirse $\sigma(m)/m = 2^{n+1}/(2^{n+1} - 1)$. La segunda fracción es irreducible y si la primera también lo fuera se tendría $\sigma(m) = 2^{n+1}$ y $m = 2^{n+1} - 1$ de donde se puede deducir que m es primo y el resultado estaría probado. Para demostrar la irreducibilidad de $\sigma(m)/m$ se emplea que $\sigma(m) = k2^{n+1}$, $m = k(2^{n+1} - 1)$ con $k > 1$ implicaría que los cuatro divisores, $1, k, 2^{n+1} - 1, m$, asociados a esta descomposición de m son

incompatibles con la condición $\sigma(m) = k2^{n+1}$ por una simple cuestión de tamaño (véase en [Di] una simplificación).

Hay una pregunta natural, y más todavía a la luz del resultado de Euler: ¿existen los números perfectos impares? Hasta la fecha el problema está abierto. Euler juzgó en [E798] el problema como 'muy difícil', también limitó las posibilidades para la factorización de estos hipotéticos números en la línea de un resultado conjeturado por R. Descartes [To]. Actualmente la combinación de trabajo computacional y teórico permite asegurar que si los números perfectos impares existieran, el primero de ellos sería gigantesco (al menos varios cientos de cifras).

Las ecuaciones $x^r \equiv 1 \pmod{n}$ que guiaron una buena parte de las investigaciones de Euler en divisibilidad están íntimamente ligadas a la estructura del grupo multiplicativo $\mathbb{Z}_n^*$ y a pesar de que Euler no alcanzó la precisión de Gauss en el análisis de estos grupos cuando todavía no existía la teoría de grupos, llegó a probar (empleando el trabajo de Lagrange) que $\mathbb{Z}_p^*$ es cíclico, es decir, la existencia de *raíces primitivas* (véase en Art. 56 de [Ga] la opinión de Gauss). El tema por el hecho de ser clásico no está acabado en la actualidad y hay una conjetura de Artin que pregunta, en una forma un poco más precisa, acerca de si cada $a \in \mathbb{Z} - \{-1, \text{cuadrados}\}$ es generador de infinitos $\mathbb{Z}_p^*$. Un resultado de D.R. Heath-Brown [HeBr] está increíblemente cerca de la conjetura. El caso $a = 10$ está relacionado con la aritmética elemental: Si n no es divisible por 2 ni por 5 es bien conocido que $1/n$ tiene un desarrollo decimal periódico puro. Con la congruencia de Euler-Fermat se puede probar que la longitud del periodo es a lo más $n-1$ y que si se alcanza, n es primo (por ejemplo esto ocurre para $n = 7$ y $n = 17$). La conjetura de Artin implicaría que hay infinitos de esos primos y que incluso tienen cierta densidad. Como pasatiempo para el lector se deja justificar que siempre para estos primos la segunda parte del periodo es el complemento a 9 de la primera parte:

$$\frac{1}{7} = 0'\overline{142\mathbf{857}}\ldots \qquad \begin{array}{r} 857 \swarrow \\ \hline 999 \end{array}$$

$$\frac{1}{17} = 0'\overline{0588235\mathbf{94117647}}\ldots \qquad \begin{array}{r} 94117647 \swarrow \\ \hline 99999999 \end{array}$$

3. Ecuaciones diofánticas

Como indica la cita mencionada en la sección introductoria, Euler extiende en [EuAl] la resolución de ecuaciones algebraicas al caso en que las soluciones están en $\mathbb{Z}$ o $\mathbb{Q}$, por ello considera allí muchos tipos de ecuaciones diofánticas.

Hoy en día podemos hacer una división en grandes bloques. Una buena parte de los problemas que trató corresponden a hallar puntos racionales en curvas proyectivas sobre $\mathbb{Q}$. El caso de grado 2 es de género 0, lo que significa que (dando por supuesto que hay un punto racional) existe una parametrización racional. Por ejemplo

$$x^2+y^2=1 \quad \longleftrightarrow \quad x=\frac{t^2-1}{t^2+1}, \quad y=\frac{2t}{t^2+1} \tag{1}$$

lo que permite hallar todas las soluciones racionales de $x^2+y^2=1$ (el punto $(1,0)$ se obtiene con $t=\infty$). El caso de grado 3 tiene típicamente género 1, es decir, es una curva elíptica (suponiendo de nuevo un punto racional). No se puede parametrizar pero el hecho de que sea isomorfa a su jacobiana se traduce en que hay una ley de grupo que permite operar los puntos racionales (un hecho anticipado por Fermat), en palabras de Euler:

> [...] sólo podemos dar reglas para aquellos casos en los cuales partamos de una solución conocida para encontrar otra nueva, por medio de la cual podemos entonces encontrar una tercera y proceder sucesivamente de la misma forma con las otras.

Para géneros superiores D. Mumford probó en 1965 [Mu] que los puntos racionales deben estar muy espaciados y finalmente G. Faltings [Fa] en 1983 demostró la *conjetura de Mordell*: que son un número finito.

Deshomogeneizando, los puntos racionales en las curvas de grado 2 o 3 como antes, están asociados a la representación de 0 por formas cuadráticas o cúbicas ternarias. Por ejemplo, la parametrización (1) da lugar a la bien conocida fórmula para las ternas pitagóricas (coprimas) $x^2+y^2=z^2$:

$$x=m^2-n^2, \qquad y=2mn, \qquad z=m^2+n^2.$$

Sin embargo si queremos hallar puntos enteros en curvas entramos en terrenos bien distintos: en el caso cuadrático se tiene la teoría de formas

cuadráticas, que trataremos más adelante, y el caso de curvas elípticas y de géneros superiores está relacionado con temas de aproximación diofántica. Un teorema de C.L. Siegel de 1929 [Si] afirma que sólo puede haber un número finito de tales puntos. Este resultado no es efectivo, no ofrece ningún algoritmo para hallarlos ni para decidir si hay alguno. Euler se refiere a esta dificultad en el caso elíptico:

> Busquemos entonces transformar la fórmula $a + bx + cx^2 + dx^3$ en un cuadrado y hallar los valores de x con este propósito expresados como números racionales. Como esta investigación cuenta con muchas más dificultades que cualquiera de los casos precedentes, se requieren más artificios para encontrar incluso valores fraccionarios y con ello estaremos satisfechos, sin pretender averiguar valores enteros.

En vez de enumerar las ecuaciones diofánticas de las que se ocupó Euler, reservaremos la próxima sección para las formas cuadráticas binarias y nos centraremos aquí en una de ellas de especial relevancia: el caso $n = 3$ del *último teorema de Fermat*.

E. Kummer

Por supuesto, el último teorema de Fermat no necesita presentación, siendo uno de los problemas matemáticos más difundidos en los últimos años debido a su curioso origen y a su reciente solución. Verdaderamente es una cita casi obligada para cualquier texto de divulgación matemática. Como síntesis brevísima de su historia (véase en [To], y con mayor extensión en [He], una discusión que abarca hasta nuestros días) recordemos que proviene de una anotación de Fermat (alrededor de 1630) en la que afirmaba que para cada $n > 2$ la ecuación

$$x^n + y^n = z^n \tag{2}$$

no tiene soluciones no triviales ($xyz \neq 0$) en enteros. El propio Fermat probó el caso $n = 4$ y, sin olvidar la contribución de S. Germain, el mayor avance general hasta el siglo XX lo hizo E. Kummer en 1847 [Ed] creando la teoría de ideales; ya en 1983 la prueba de la conjetura de Mordell por Faltings [Fa] permitió concluir (mediante técnicas de geometría aritmética en variedades abelianas) que para cada n sólo puede

haber un número finito de soluciones (primitivas) de (2); un resultado poco divulgado de L.M. Adleman y Heath-Brown [AdHB], basado en un trabajo anterior de E. Fouvry, implica que para infinitos exponentes no hay solución en el llamado *primer caso*; finalmente A. Wiles dio la prueba definitiva [Wi] estableciendo una sorprendente relación, conjeturada años atrás, entre la teoría de curvas elípticas y la de formas modulares (mucho más importante que el último teorema de Fermat en sí, que en gran medida es un resultado anecdótico catapultado por su va lor histórico).

Euler probó de nuevo el caso $n = 4$ y su contribución original fue el caso $n = 3$. Su demostración tiene una laguna sutil, que también aparece ocasionalmente cuando estudia formas cuadráticas, pero que él podría haber completado (por ello prácticamente nunca se le deja de atribuir este caso del último teorema de Fermat). La prueba y la propia laguna tienen gran interés para la posterior evolución de la teoría algebraica de números, por ello respetaremos con cierta fidelidad los pasos principales dados por Euler tal como aparecen en el capítulo XV de [EuAl].

En la Cuestión 1, plantea el problema: "Se requiere encontrar dos cubos, x^3 e y^3, cuya suma sea un cubo". En primer lugar Euler intenta sin éxito una especie de parametrización de la curva elíptica $x^3+1 = y^3$ obtenida al deshomogeneizar (2) para $n = 3$, como no puede hacerlo escribe: "por tanto podemos inferir, con cierto grado de certeza, que es imposible encontrar dos cubos cuya suma sea un cubo. Pero estaremos totalmente convencidos con la siguiente demostración". Ciertamente este comentario y el análisis que no conduce a la solución difícilmente aparecerían en un texto de matemáticas actual pero son indudablemente ilustrativos y didácticos.

La demostración a la que se refiere trata de proceder como en el método del descenso de Fermat: se parte de una hipotética solución no trivial de $x^3+y^3 = z^3$ y se construye a partir de ella otra 'menor', como el proceso no se puede continuar indefinidamente, se llega a una contradicción. Lo primero que hace Euler es escribir $x = p+q$, $y = p-q$, con $4|p$ y p y q coprimos. Este cambio de variable viene motivado por la factorización de $x^3 + y^3$ y con él la ecuación se transforma en

$$2p \cdot (p^2 + 3q^2) = z^3.$$

Suponiendo $3 \nmid p$ (el caso $3|p$ se trata aparte) se puede demostrar que $2p$ y p^2+3q^2 son coprimos. Por razones poco claras, Euler divide ambos miembros por 8 (esto es irrelevante) y hace la afirmación absolutamente irreprochable:

> Para que el producto $p/4 \cdot (p^2 + 3q^2)$ pueda ser un cubo, cada uno de estos factores, a no ser que tenga un factor común, deben ser un cubo cada uno.

La genialidad de Euler es descomponer $p^2 + 3q^2$ como

$$(p + q\sqrt{-3})(p - q\sqrt{-3}),$$

un truco que empleó en otros contextos, por supuesto los factores no son números enteros, ni siquiera reales pero, y aquí está la laguna, Euler con visión profética aplica la observación anterior:

> Para que p^2+3q^2 sea un cubo, sólo tenemos que suponer, como hemos visto antes $p \pm q\sqrt{-3} = (t \pm u\sqrt{-3})^3$.

Con esta relación se puede concluir:

$$2p = 2t(t + 3u)(t - 3u)$$

pero como $2p$ es un cubo y se puede probar que los factores son coprimos, tendremos $2t = h^3$, $t + 3u = f^3$, $t - 3u = g^3$ y esto da lugar a la nueva solución $h^3 = f^3 + g^3$ y se puede probar que es más pequeña que la inicial (intuitivamente, t y u son como raíces cúbicas de p).

El paso sospechoso en el argumento de Euler está relacionado con la factorización única en anillos de enteros algebraicos (véase la siguiente sección) y lo que la salva es que $\mathbb{Z}[(1 + \sqrt{-3})/2]$ es de factorización única. Por supuesto que esta nomenclatura y esta orientación quedan lejos de las Matemáticas del siglo XVIII pero con un lenguaje diferente el resultado es asequible con los métodos de Euler (de hecho está muy relacionado con [E272]).

4. Formas cuadráticas

Dentro de las formas cuadráticas binarias, Euler se preocupó especialmente por $x^2 + ny^2$, las que hoy llamaríamos del género principal. Leyendo [EuAl] no es difícil imaginar el motivo para tal restricción: completando cuadrados $ax^2 + bxy + cy^2$ se escribe como $\alpha x^2 + \beta y^2$

y multiplicando por α o por β un nuevo cambio de variable lleva a x^2+ny^2. Por supuesto que estos cambios no son invertibles en los enteros y esta simplificación pierde gran parte de la teoría de formas cuadráticas pero todavía alberga una riqueza inusitada.

El tipo de problemas de los que ocupó Euler a este respecto continúan los intereses de Fermat y esencialmente se centran en la representación de enteros por x^2+ny^2 y sobre todo en las propiedades de divisibilidad de los números representados. No es difícil imaginar a Fermat y a Euler jugando con estos problemas de sencillo enunciado, fáciles de contrastar experimentalmente y que escapaban a veces a sus geniales habilidades.

Por comenzar con uno de los ejemplos más sencillos que ambos supieron abordar, al factorizar los números de la forma x^2+y^2 con x e y coprimos resulta que siempre se obtienen primos de la forma $p=4n+1$ o $p=2$, por ejemplo $8^2+1^2=5\cdot 13$, $14^2+5^2=13\cdot 17$, $1^2+7^2=2\cdot 5^2$.

De ello se puede deducir el hecho nada trivial de que hay infinitos primos de la forma $4n+1$ porque dados $p_1,\dots,p_k$ de este tipo, los factores primos de $(2p_1p_2\dots p_k)^2+1^2$ añaden elementos nuevos a la lista. Además, un primo impar se puede escribir como suma de dos cuadrados si y sólo si es de la forma $4n+1$ [E228].

Otras propiedades similares y más complejas se observan en otras formas cuadráticas del mismo tipo, por ejemplo los números x^2+5y^2 con x e y coprimos sólo pueden tener como factores primos $p=2$, $p=5$ o en alguna de las cuatro progresiones artiméticas $20n+1$, $20n+3$, $20n+7$, $20n+9$ (Teorema 10 de [E164]) pero un primo ($p\neq 2,5$) se puede escribir como x^2+5y^2 si y sólo si pertenece a la primera o a la última progresión. Aunque este enunciado involucre sólo las operaciones de la aritmética elemental, de ninguna manera es sencillo.

Euler hace de [E164] una declaración de intenciones para sus investigaciones futuras recopilando una lista de hasta 59 "teoremas" experimentales (en una carta a Goldbach reconoció que no tenía las pruebas) y diversos comentarios al respecto. Allí está por ejemplo una forma parcial de la *ley de reciprocidad cuadrática*, el enunciado completo aparece en [E552] (véase el comentario en [Le]), esta ley es uno de los resultados más notables de la teoría de números. Para enunciarla en su forma actual es conveniente definir el *símbolo de Legendre* para cada p primo

y $p \nmid N$

$$\left(\frac{N}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv N \pmod{p} \text{ tiene solución} \\ -1 & \text{si } x^2 \equiv N \pmod{p} \text{ no tiene solución} \end{cases}$$

En el primer caso se dice que N es un *residuo cuadrático* módulo p. La ley de reciprocidad cuadrática afirma que si p y q son primos impares distintos entonces

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

y se completa con las leyes suplementarias

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad \text{y} \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Esto es totalmente inesperado y además profundo. Hubo que esperar muchos años hasta que Gauss diera una prueba.

Para ilustrar la aplicación de la ley de reciprocidad cuadrática mediante un ejemplo, consideremos la afirmación de Euler en el Teorema 10 de [E164], que ya hemos citado antes, diciendo que los divisores primos de x^2+5y^2 (con x e y coprimos) están en las progresiones $20n+1$, $20n+3$, $20n+7$, $20n+9$, aparte de los casos $p = 2$ y $p = 5$. En notación moderna lo que se requiere es $x^2+5y^2 \equiv 0 \pmod{p}$. Multiplicando por el inverso de y^2 módulo p, se tiene $z^2 + 5 \equiv 0 \pmod{p}$, es decir, que -5 es un residuo cuadrático módulo p. Como Euler sabía, el símbolo de Legendre es multiplicativo, con ello y la ley de reciprocidad cuadrática tenemos que

$$1 = \left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{5}\right).$$

Requiere un breve cálculo comprobar que los únicos residuos cuadráticos módulo 5 son los elementos de las clases de 1 y -1 (son congruentes a 1^2 y a 2^2), por consiguiente p debe cumplir o bien $(-1)^{(p-1)/2} = 1$ y $p \equiv \pm 1 \pmod{5}$, o bien $(-1)^{(p-1)/2} = -1$ y $p \not\equiv \pm 1 \pmod{5}$, lo cual da lugar a las progresiones de la afirmación de Euler.

Una vez que uno conoce que $\mathbb{Z}_p^*$ es cíclico, se deduce que los elementos de orden par son justamente las soluciones de $x^{(p-1)/2} = 1$ en este grupo. Con ello se llega al conocido *criterio de Euler* que en notación moderna se escribe

$$\left(\frac{N}{p}\right) \equiv N^{(p-1)/2} \qquad \text{para } p \text{ primo impar } p \nmid N.$$

Nótese que la primera de las leyes suplementarias es consecuencia inmediata.

Los problemas de representación por formas cuadráticas son más complejos que los de divisibilidad. Euler tuvo éxito en los casos x^2+y^2, x^2+2y^2 y x^2+3y^2, y curiosamente se acercó a otros con un propósito que podría decirse computacional, en relación con algoritmos de primalidad. Antes de entrar en ello, veamos un escollo delicado incluso en un ejemplo sencillo.

P.G.L. Dirichlet

La ecuación $x^2+y^2=13$ tiene una única solución en enteros, 3^2+2^2, salvo las simetrías de la ecuación ($x \mapsto \pm x$, $y \mapsto \pm y$, $x \leftrightarrow y$). Podríamos explicar esto en la línea del punto sospechoso de la prueba de Euler del último teorema de Fermat para $n=3$, diciendo que $13=(3+2i)(3-2i)$ y que (salvo signos) sólo hay una forma de escribir esto como

$$(x+iy)(x-iy)$$

que conduce a la solución $x+iy=3+2i$. Aquí $3\pm 2i$ son "primos" en el sentido de que no se pueden descomponer de manera no trivial como $(a+bi)(c+di)$. Si tratamos de aplicar el mismo razonamiento a $x^2+5y^2=21$ tenemos que $21=(1+2\sqrt{-5})(1-2\sqrt{-5})$ con $1\pm 2\sqrt{-5}$ "primos" en el sentido anterior, sin embargo además de la solución $1^2+5\cdot 2^2=21$ se tiene otra, $4^2+5\cdot 1^2=21$, que no tiene nada que ver con esta descomposición. La razón de este comportamiento peculiar es que en la segunda ecuación la factorización en "primos" no es única, por ejemplo $3\cdot 7=(1+2\sqrt{-5})(1-2\sqrt{-5})$ y ¡todos los factores son irreducibles! Con un lenguaje actual, lo que ocurre es que $\mathbb{Z}[i]$ es un dominio de factorización única y $\mathbb{Z}[\sqrt{-5}]$ no lo es. La teoría de ideales nos permite reestablecer la analogía definiendo números literalmente ideales que expresan por ejemplo lo que tienen en común 3 y $1\pm 2\sqrt{-5}$ o 7 y $1\pm 2\sqrt{-5}$ para dar una descomposición más fina que siempre es única. El paso de los números "ideales" a los "reales" está regulado por cierto grupo abeliano finito, el *grupo de clases*, cuyos elementos están

asociados a clases de formas cuadráticas y cuyo orden se expresa en términos de los caracteres reales de cierto $\mathbb{Z}_n^*$ a través de la *fórmula del número de clases* probada por P.G.L. Dirichlet.

La limitación en el tipo de formas cuadráticas que consideraba Euler y los márgenes de las Matemáticas de su tiempo dejaron fuera de su alcance toda la extensión del problema de representación. Sin embargo hay un tema de profundidad notoria en lo que se llama, siguiendo a Euler, *números convenientes* o *números idóneos*. El punto de partida es que un número $N = 4n + 1$ es primo si y sólo si se puede escribir de forma (esencialmente) única como $N = x^2 + y^2$, esto conduce a un algoritmo efectivo de primalidad y de factorización. Euler estudió los valores de n para los cuales nx^2+y^2 tiene una propiedad similar [E498], textualmente:

> Todos los números contenidos de una sola forma en x^2+y^2 son primos o dobles de primos donde x e y son primos entre sí. He observado que otras expresiones similares de la forma $nx^2 + y^2$ gozan de la misma propiedad dando a la letra n valores *convenientes*.

(En realidad hay que leer entre líneas para tener una definición coherente [We]). Euler obtuvo un criterio para detectarlos (véase en [Ed] la curiosa historia de su prueba) y dio una tabla de 65 de tales números que empleó efectivamente para fabricar algunos primos grandes. Hoy en día podemos traducir todo esto en términos de propiedades del grupo de clases (los números convenientes ocurren si cada género sólo tiene una clase) [Co]. Además W.E. Briggs y S. Chowla [BrCh] probaron en 1954 que en la tabla de Euler falta a lo más un número y que si tal número existiera debería tener al menos varias decenas de cifras.

Respecto a las formas cuadráticas binarias indeterminadas, el interés de Euler por la ecuación de Pell se manifiesta en varios de sus trabajos [E29], [E279], [E323], [EuAl], etc. Uno de los más relevantes es [E323] donde aparece la solución en términos de fracciones continuas. Con la notación actual, los coeficientes de la fracción continua de x son $a_n = [x_n]$ con $x_0 = x$ y $x_{n+1} = (x_n - [x_n])^{-1}$. Para $\sqrt{N}$ la sucesión de coeficientes es periódica. A partir de los coeficientes se construyen las

convergentes p_n/q_n con p_n y q_n definidos recurrentemente por

$$p_n = a_n p_{n-1} + p_{n-2},\ p_{-1} = 1,\ p_0 = a_0,\ \text{y}$$
$$q_n = a_n q_{n-1} + q_{n-2},\ q_{-1} = 0,\ q_0 = 1.$$

La menor solución en enteros positivos de la ecuación $x^2 - Ny^2 = 1$ es $(x, y) = (p_{n_0}, q_{n_0})$ donde n_0 tiene que ver con el periodo de los a_n (n_0+1 es el periodo o su doble). Por ejemplo, para $N = 13$ la sucesión $\{a_n\}$ es $3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, \ldots$ que lleva a la solución $(x, y) = (p_9, q_9) = (649, 180)$ de $x^2 - 13y^2 = 1$.

Antes de concluir esta sección es justo mencionar que los intereses de Euler se extendieron también a algunas formas cuadráticas no binarias por ejemplo a través de la fascinación por la conjetura de Fermat de que todo número se puede representar como suma de tres números triangulares (los de la forma $n(n+1)/2$) y como suma de cuatro cuadrados. Lo primero fue probado por Gauss y lo segundo por Lagrange (con una enorme simplificación inmediatamente posterior de Euler [Di]).

5. Los albores de la teoría analítica de números

Euler, de quien F. Arago dijo "podría haber sido llamado, casi sin metáfora y ciertamente sin hipérbole, la encarnación del análisis", conjugó su genialidad en análisis y en teoría de números para dar los primeros pasos en lo que más tarde se llamaría teoría analítica de números, una disciplina cuyo nacimiento en toda regla se suele fechar en 1837 con el trabajo de Dirichlet.

En 1737, en la segunda parte de [E72] Euler establece la fórmula

$$\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdot\cdots\cdot\frac{p}{p-1}\cdot\cdots = \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\ldots \tag{3}$$

donde p recorre los primos. Ciertamente esta igualdad desazona al lector actual porque la serie del segundo miembro es divergente. Para nuestra tranquilidad poco después escribe una identidad que utilizando la notación de Riemann $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ es

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}. \tag{4}$$

Esto es lo que se llama *producto de Euler* para $\zeta(s)$ o *identidad de Euler* (pero hay tantas identidades de Euler...), formalmente (3) es el caso $s = 1$ de (4). La demostración es elemental e ingeniosa:

$$\zeta(s)(1 - 2^{-s}) = \zeta_2(s),$$

donde $\zeta_2(s)$ es como $\zeta(s)$ pero restringiendo la sumación a los impares, es decir, a $\mathrm{mcd}(n, 2) = 1$. De la misma forma

$$\zeta(s)(1 - 2^{-s})(1 - 3^{-s}) = \zeta_2(s) - 3^{-s}\zeta_2(s) = \zeta_6(s),$$

donde la sumación en $\zeta_6(s)$ se restinge a los n con $\mathrm{mcd}(n, 6) = 1$. Iterando se deduce, para $s > 1$, que

$$\zeta(s)(1 - 2^{-s})(1 - 3^{-s}) \dots (1 - p^{-s}) \to 1 \text{ cuando } p \to \infty$$

porque 1 es el único número natural que no es divisible por ningún primo.

¿Por qué (4) es algo más que una identidad curiosa? ¿qué la diferencia por ejemplo de $\pi = 4\sum_{k=1}^{\infty}(-1)^{k+1}/(2k-1)$? Para responder es pertinente usar las palabras de Hardy cuando en §11 [Ha] justifica la seriedad y belleza de los teoremas matemáticos:

> Se puede decir aproximadamente que una idea matemática es 'significante' si se puede conectar, de manera natural y esclarecedora, con un gran complejo de otras ideas matemáticas.

Por supuesto que conectar π con los inversos de los impares es inesperado y se puede utilizar para deducir otros resultados pero esta conexión es débil en comparación con la que expresa la identidad de Euler (4): en un lado tenemos los primos (aparentemente caóticos) y en el otro los naturales (el prototipo de orden), y además hay una variable que se puede acercar a voluntad a la singularidad para dar mayor importancia a los términos lejanos de la series. Con ello se crea una relación básica entre la aritmética y el análisis.

El primer uso que dio Euler a (4) es una prueba de la infinitud de los primos. Hoy en día tomaríamos $s \to 1^+$ en (4) pero cualquiera que haya disfrutado de la lectura de [EuIn] sabrá que Euler no se arredraba ante los infinitos y trabajó directamente con (3), como el segundo miembro es ∞ el primero debe serlo y por tanto no puede haber un número finito de primos. ¿Qué pensaría Euclides de esta prueba? En realidad Euler establece su resultado de una forma más (¿o menos?) precisa y afirma

que $\prod(1-p^{-1})^{-1} = \log\infty$ donde "$\log\infty$ es el mínimo entre todas las potencias de infinito".

Otro conclusión que extrajo es que "Los primos son infinitamente más numerosos que los cuadrados" porque $\prod(1-n^{-2})^{-1} = 2$. Si los primos crecieran tan deprisa o más que los cuadrados, deberíamos tener $\infty = \zeta(1) < 2$. Con la lógica aplastante de $\log\infty < \infty$ y $\prod(1-n^{-1})^{-1} = \infty$, concluye también que "Los primos son infinitamente menos numerosos que los naturales". Hoy en día probaríamos que $\prod(1-n^{-1})^{-1}/\zeta(s) \to \infty$ cuando $s \to 1^+$.

El resultado más importante que alcanzó en esta línea es que la suma de los inversos de los primos diverge aunque muy lentamente, para él la suma es sólo de tamaño $\log\log\infty$ (véase en [Du] una prueba completamente satisfactoria para el lector moderno).

La importante conclusión de todo esto es que gracias a (4) se puede establecer una relación entre el crecimiento de los primos y el comportamiento de una función, $\zeta(s)$. Euler también construyó variantes de los argumentos anteriores para tratar primos en algunas progresiones aritméticas, especialmente los de la forma $4n+1$, pero hasta Dirichlet no se pudieron integrar dentro de un mismo marco para probar un resultado general.

El tema de la distribución de los primos permaneció durante todo el siglo XIX y cabe citar los resultado de Chebychev [Sm] (quien por cierto participó en la edición en 1849 de los trabajos de Euler sobre teoría de números) que se acercaban al *teorema de los números primos* que Gauss había conjeturado tras unos extensos cálculos en la forma:

$$\pi(x) \sim \int_2^x \frac{dt}{\log t} \qquad \text{con } \pi(x) = \#\{p \le x\}. \tag{5}$$

De hecho, numéricamente esta aproximación tiene un error relativo notablemente pequeño.

El gran salto vino con Riemann que en su celebérrima y brevísima memoria de 1859 (véase [Ri] p. 79–86) 'despejó' $\pi(x)$ de (4) en términos de los ceros de la extensión meromorfa de $\zeta(s)$ al plano complejo. Es más sencillo escribir el resultado poniendo algunos pesos al contar los

primos:

$$\sum_{p^m \leq x} \log p = x - \frac{\zeta'(0)}{\zeta(0)} - \sum_{\rho} \frac{x^\rho}{\rho}$$

donde ρ recorre los ceros de (la extensión meromorfa de) ζ y por razones técnicas $x \notin \mathbb{Z}$. Esta fórmula no se puede aprovechar si no tenemos cierto control sobre ρ y sobre la convergencia de la serie, sobre cuándo la podemos truncar. Éste es un tema delicado que Riemann no trató por completo, por ello la prueba de (5), en una forma un poco más precisa no llegó hasta 1896, con los trabajos independientes de Hadamard y de la Vallée Poussin.


B. Riemann

Cuanto menor sea $\Re\rho$, menor es la contribución de la serie infinita anterior para x grande, lo que se traduce en un menor error en (5). Se sabe por cierta ecuación funcional (también relacionada con el trabajo de Euler) que si ρ es un cero con $\Re\rho > 0$, entonces $1-\rho$ también lo es, por consiguiente la mejor situación se daría bajo la llamada *Hipótesis de Riemann*: Todos los ceros ρ en $\Re\rho > 0$ satisfacen $\Re\rho = 1/2$. Éste antiguo e importante problema permanece abierto. En caso de que la afirmación fuera correcta, se podría deducir

$$\pi(x) \sim \int_2^x \frac{dt}{\log t} + O(\sqrt{x}\log x).$$

La relación analítico-aritmética funciona en los dos sentidos: la fórmula anterior es cierta si y sólo si se cumple la hipótesis de Riemann. Es decir, conocer la distribución de los primos equivale a saber si los ceros de cierta función meromorfa están en fila india. Una relación que, con toda seguridad, hubiera hecho las delicias de Euler.

Agradecimientos: Quisiera expresar mi gratitud a A. Río y a S. Xambó por la invitación y su atenta amabilidad, así como a A. Ubis por sus acertadas sugerencias. También quisiera agradecer especialmente el apoyo de E. Valenti.

Referencias[5]

[AdHB] L.M. Adleman; D.R. Heath-Brown. *The first case of Fermat's last theorem.* Invent. Math. 79 (1985), no. 2, 409–416.

[AGP] W.R. Alford, A. Granville, C. Pomerance. *There are infinitely many Carmichael numbers.* Ann. of Math. (2) 139 (1994), no. 3, 703–722.

[BrCh] S. Chowla; W.E. Briggs. *On discriminants of binary quadratic forms with a single class in each genus.* Canadian J. Math. 6, (1954), 463–470.

[Co] D.A. Cox. *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication.* A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[Da] *The Euler archive.* `http://www.math.dartmouth.edu/~euler/` .

[Di] L.E. Dickson. *History of the theory of numbers.* Vol. I,II,III. Chelsea Publishing Co., New York 1966.

[Du] W. Dunham. *Euler. El maestro de todos los matemáticos.* Nivola 2000.

[Ed] H.M. Edwards. *Fermat's last theorem. A genetic introduction to algebraic number theory.* Graduate Texts in Mathematics, 50. Springer-Verlag, New York-Berlin, 1977.

[EuAl] L. Euler. *Elements of Algebra.* New York Springer-Verlag, 1984.

[EuIn] L. Euler. *Introduction to analysis of the infinite.* Book I. Springer-Verlag, New York, 1988. (*Introducción al análisis de los infinitos* [Traducido por José Luis Arantegui Tamayo y anotado por Antonio José Durán Guardeño]. Real Sociedad Matemática Española, Madrid, 2000).

[E54] L. Euler. *Theorematum quorundam ad numeros primos spectantium demonstratio.* (Traducido al inglés por D. Zhao).

[E29] L. Euler. *De solutione problematum diophanteorum per numeros integros.* (Traducido al inglés por D. Otero).

[E72] L. Euler. *Variae observationes circa series infinitas.* (Traducido al inglés por P. Viader y L. Bibiloni).

[E134] L. Euler. *Theoremata circa divisores numerorum.* (Traducido al inglés por D. Zhao).

[E164] L. Euler. *Theoremata circa divisores numerorum in hac forma paa $\pm$ qbb contentorum.* (Traducido al inglés por J. Bell).

[E228] L. Euler. *De numeris, qui sunt aggregata duorum quadratorum.*

[E271] L. Euler. *Theoremata arithmetica nova methodo demonstrata.*

[E272] L. Euler. *Supplementum quorundam theorematum arithmeticorum, quae in nonnullis demonstrationibus supponuntur.*

[E279] L. Euler. *De resolutione formularum quadricarum indeterminatarum per numeros integros.*

[E283] L. Euler. *De numeris primis valde magnis.*

[E323] L. Euler. *De usu novi algorithmi in problemate Pelliano solvendo.*

[5]En las referencias de los artículos de Euler seguimos la numeración de Eneström. Todas ellas se pueden consultar en [Da]. En el caso de que se hayan usado traducciones, se indican los traductores.

[E369] L. Euler. *Quomodo numeri praemagni sint explorandi, utrum sint primi necne.*

[E498] L. Euler. *Extrait d'un lettre de M. Euler a M. Beguelin en mai 1778.*

[E552] L. Euler. *Observationes circa divisionem quadratorum per numeros primos.*

[E792] L. Euler. *Tractatus de numerorum doctrina capita sedecim, quae supersunt.*

[E798] L. Euler. *De numeris amicibilibus.*

[Fa] G. Faltings. *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. 73 (1983), no. 3, 349–366.

[Ga] C.F. Gauss. *Disquisitiones arithmeticae.* Springer-Verlag, New York, 1986. (*Disquisicions aritmètiques* [traducido al catalán por G. Pascual Xufré]. Institut d'Estudis Catalans, Societat Catalana de Matemàtiques, Barcelona 1996).

[Ha] G.H. Hardy. *A Mathematician's Apology.* Cambridge University Press. Canto 2001. (*Autojustificación de un matemático* [traducido por Domènec Bergadà]. Ariel, Barcelona 1981. *Apología de un matemático.* Nivola, Madrid 1999).

[HeBr] D.R. Heath-Brown. *Artin's conjecture for primitive roots.* Quart. J. Math. Oxford Ser. (2) 37 (1986), 27–38.

[He] Y. Hellegouarch. *Invitation to the mathematics of Fermat-Wiles.* Academic Press, Inc., San Diego, CA, 2002.

[Le] F. Lemmermeyer. *Reciprocity laws. From Euler to Eisenstein.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[Mu] D. Mumford. *A remark on Mordell's conjecture.* Amer. J. Math. 87 (1965), 1007–1016.

[Ri] B. Riemann. *Riemanniana Selecta* (edición, estudio introductorio y notas de José Ferreirós). Colección Clásicos del Pensamiento. Madrid, CSIC, 2000.

[Sa] E. Sandifer. *Ed Sandifer's How Euler Did It.* The Mathematical Association of America. `http://www.maa.org/news/howeulerdidit.html`.

[Si] C.L. Siegel. *Über einige Anwendungen Diophantischer Approximationen.* Abh. Preussischen Akademie der Wissenschaften, Phys. Math. Klasse (1929), 41-69.

[Sm] D.E. Smith. *A source book in mathematics.* New York: Dover Publications, 1959.

[Su] J. Suzuki. *Euler and Number Theory: A Study in Mathematical Invention.* In "Leonhard Euler: Life, Work and Legacy". R.E. Bradley, C.E. Sandifer (Ed.). Elsevier, 2007.

[To] B. Torrecillas Jover. *Fermat. El mago de los números.* Nivola 1999.

[We] A. Weil. *Number theory. An approach through history. From Hammurapi to Legendre.* Birkhäuser Boston, Inc., Boston, MA, 1984.

[Wi] A. Wiles. Modular elliptic curves and Fermat's last theorem. Ann. of Math. (2) 141 (1995), no. 3, 443–551.