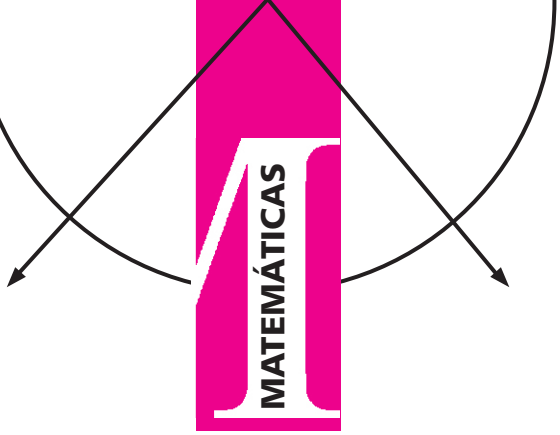
Euler, árbitro de controversias



Antonio Antolín Fonseca
antolin.antonio@gmail.com
Universidad Autónoma de Ciudad Juárez

"Pido a Dios lo preserve, querido Profesor Euler"
-Estanislao II Augusto, rey de Polonia.

En un siglo —el dieciocho— "en el que la matemática era considerada, casi sin excepción, como la cumbre del saber, el nombre de Leonhard Euler era mejor conocido que el de los genios literarios y musicales, como Swift y Bach, por ejemplo. En el firmamento de las letras sólo Voltaire brilló más que Euler" [1, p. viii]. Los reyes no desdeñaban escribir a Euler, a veces de su puño y letra [2, p. 23].

En nuestro propio siglo la matemática no ocupa ya, sin duda, el lugar privilegiado que ocupó en el Siglo de Euler, pues de este matemático prodigioso sólo se acuerda ya una parte muy pequeña de la sociedad: la comunidad de los matemáticos de profesión. Más aún, cuando pide uno a los miembros de esa comunidad que nombren a sus antepasados más ilustres, notará que pocos incluyen a Euler entre sus héroes si la lista es corta. Hay en esto una injusticia y espero que al terminar esta nota el lector concuerde conmigo.

El pasado 20 de abril, con cinco días de retraso pese a la proverbial puntualidad suiza, tuvo lugar en la Martinskirche, la iglesia más antigua de Basilea —data del año 1100 y es protestante desde 1529— una celebración del tricentésimo aniversario del nacimiento de Euler, con invitados de las academias a las que perteneció y música compuesta para la ocasión. En la Martinskirche fue bautizado a los dos días de nacido el pequeño Leonhard, hijo de Paul Euler, pastor de la iglesia de Reihen, villa del cantón de Basilea, y de su esposa Marguerite, cuyo apellido de soltera era Brucker. El apellido Brucker gozaba de cierta distinción en la república de las letras [2, p. 2]. Sirva también esta nota como una muy modesta celebración del natalicio de este Leonardo, cuya fama debiera rivalizar con la del otro.

Hablar de Euler exige superlativos. Es el matemático más prolífico de la historia: alrededor de una tercera parte de las publicaciones de investigación en matemáticas, física matemática e ingeniería mecánica de los últimos tres cuartos del siglo dieciocho son de Euler. Desde 1729 en adelante, hasta 50 años después de su muerte, los artículos de Euler llenaron la mitad de las páginas publicadas por la Academia de San Petersburgo; además, desde 1746 a 1771, trabajos de Euler ocuparon también la mitad de las memorias científicas de la Academia de Berlín. Escribió también para otras publicaciones periódicas, amén de entregar colecciones de artículos a libreros para la publicación de volúmenes constituidos exclusivamente por sus trabajos [1, pp. viii–ix]. En esta vasta producción no hay apenas repeticiones, excepto por razones didácticas. Incluso sus libros de texto —alrededor de 25— suelen estar repletos de resultados originales.

La mera magnitud de la obra euleriana no debe agotar los superlativos: la calidad de la misma los demanda igualmente. Mencionemos de entrada dos indicadores de dicha calidad, uno contemporáneo de Euler y otro que, por ser contemporáneo nuestro, apunta a la vigencia de su obra: Euler ganó doce veces —trece según Condorcet [3, p. 15]— el codiciado premio de la Academia de Ciencias de París; su obra continúa siendo citada en publicaciones científicas no históricas [1,p. x]. Pero estas son medidas burdas. Intentaré, hasta donde mis limitaciones lo permitan, dar una mejor idea de la importancia de Leonhard Euler, el matemático.

Digo Euler, el matemático, pues conviene recordar que amén de ser, indiscutiblemente, el mayor matemático del siglo dieciocho, Euler es también el mejor físico del mismo siglo. Cedo la palabra a Truesdell:

> Euler fue el primero en obtener la ecuación de estado de un gas a partir de una teoría cinético-molecular [indicando el camino a la termodinámica de un siglo después]. En óptica geométrica inventó la lente acromática [potenciando así la observación astronómica]. Su diseño requería lentes de una calidad elevada, definida y reproducible; los intentos de fabricar lentes de acuerdo a sus especificaciones actuaron, según algunos, como estímulo en el surgimiento de la industria óptica en Alemania, cuya precisión reinó suprema durante un siglo al menos. Diseñó e hizo construir un aparato para medir el índice de refracción de un líquido; funcionó y permaneció en uso durante centuria y media. La hidrodinámica de Euler fue la primera teoría de campo [las ecuaciones de Navier - Stokes no se oponen, sino que generalizan a las suyas]. Tal vez su avance más importante en física, fuera de la mecánica, es el haber tomado el hecho observado de que los rayos de luz se cruzan sin interactuar como justificación del empleo de su teoría lineal de campo de las ondas acústicas para describir ondas de luz en un éter luminífero, el cual visualizaba como un fluido sutil, [lo que corrobora nuestra sospecha de que Euler empezó a hacer en el siglo dieciocho la física del diecinueve; recordemos que la idea del éter, ese sutil fluido que permea el Universo, no fue abandonada sino en las primeras décadas del siglo veinte, cuando los físicos aceptaron el revolucionario análisis einsteniano del experimento de Michelson y Morley] [1, p. x–xi]. La mayor parte de los principales avances globales del siglo entero fueron efectuados por [Euler], habiendo resuelto, además, numerosos pro-

blemas clave y centenares de ejemplos [1, p.xiv].

Las contribuciones de Euler a la mecánica "rebasan los superlativos". Alrededor de la mitad de su obra se ocupa directamente o indirectamente de la mecánica nos dice Truesdell —uno de los editores de las Opera Omnia de Euler; aunque según estadísticas de Youschkevitsch —otro de los editores— sólo el 28 % de su obra debe clasificarse como perteneciente a la mecánica o la física [4 ,p.15]. No hay aquí contradicción alguna: mucha de la matemática de Euler tiene su origen en problemas mecánicos. Aquí nuevamente no es la mera cantidad lo que permite aquilatar el valor de la contribución de Euler. El haber emancipado a la mecánica de las limitaciones del lenguaje geométrico, imbuyéndola de análisis [3, p. 12], junto con su genio e inagotable energía, permitió a Euler reformular la disciplina simplificándola a la vez que generalizándola, aplicándola a nuevas situaciones, resolviendo los problemas planteados por sus antecesores, unificando áreas que habían parecido ajenas hasta entonces [1, p. xvii]. Euler es el segundo Newton y sin él la labor del primero habría quedado trunca.

Es momento de hablar de las matemáticas de Euler. Empezaré por el así llamado Problema de Basilea: encontrar la suma

$$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots$$

de los recíprocos de los cuadrados de los números naturales. Planteado ya por Pietro Mengoli (1626 – 1686), discípulo de Torricelli, fue atacado por los miembros más eminentes del clan Bernoulli, nativos de Basilea: Jakob (1654 – 1705), Johann (1667 – 1748) y Daniel (1700 – 1782), así como por Gottfried Wilhelm Leibniz (1646 – 1716), James Stirling (1692 – 1770) y Abraham de Moivre (1667 – 1754), sin éxito. El problema fue resuelto finalmente por el más ilustre basileano, Leonhard Euler; haber triunfado, joven aún —contaba 27 años— donde algunos de los más grandes matemáticos de previas generaciones fracasaron, consolidó el prestigio de Euler, académico en San Petersburgo. Siete años después, en 1741, Euler encontró una segunda solución. La mejor conocida es la de 1734 y aquí presentaré ambas en orden cronológico(ver [4, cap. 3] y [5]).

Recordemos el desarrollo del seno en serie de potencias alrededor de $x=0$:

$$\operatorname{sen} x = x-\frac{x^3}{3!}+\frac{x^5}{5!}-\frac{x^7}{7!}+\cdots$$

Obtenemos de aquí

$$\frac{\operatorname{sen} x}{x}=1-\frac{x^2}{3!}+\frac{x^4}{5!}-\frac{x^6}{7!}+\cdots$$

Euler trata, como le es natural, esta serie como un polinomio de grado infinito. Ahora bien, un polinomio se descompone en factores lineales correspondientes a sus raíces y dos polinomios que tienen las mismas raíces sólo pueden diferir en un factor constante; luego, si dos polinomios que tienen las mismas raíces toman el mismo valor distinto de cero al evaluarlos en un mismo punto, serán idénticos. Los "polinomios"

$$1-\frac{x^2}{3!}+\frac{x^4}{5!}-\frac{x^6}{7!}+\cdots$$

y

$$\begin{aligned}(1-\frac{x}{\pi})(1-\frac{x}{-\pi})(1-\frac{x}{2\pi})(1-\frac{x}{-2\pi})\cdot\\ \cdot(1-\frac{x}{3\pi})(1-\frac{x}{-3\pi})\cdots\\ =(1-\frac{x^2}{\pi^2})(1-\frac{x^2}{4\pi^2})(1-\frac{x^2}{9\pi^2})\cdots\end{aligned}$$

tienen las mismas raíces $x=n\pi$, donde n es un entero distinto de cero; además ambos valen 1 en $x=0$, es decir, que

$$1-\frac{x^2}{3!}+\frac{x^4}{5!}-\frac{x^6}{7!}+\cdots=(1-\frac{x^2}{\pi^2})(1-\frac{x^2}{4\pi^2})(1-\frac{x^2}{9\pi^2})\cdots$$

No es difícil ver que el coeficiente de x^2 en el miembro derecho de esta igualdad es

$$-(\frac{1}{\pi^2}+\frac{1}{4\pi^2}+\frac{1}{9\pi^2}+\cdots)$$

mientras que en el lado izquierdo x^2 aparece con coeficiente $-\frac{1}{3!}$, de modo que

$$\frac{1}{\pi^2}+\frac{1}{4\pi^2}+\frac{1}{9\pi^2}+\cdots=\frac{1}{6}$$

o

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

Si viviera mi hermano!, exclamó Johann Bernoulli.

La segunda solución que dio Euler al Problema de Basilea no involucra productos infinitos. Apareció en 1743 en el Journal littéraire dÁllemagne, de Suisse et du Nord, que se publicaba en La Haya y es como sigue:

Sea s la longitud de arco en el círculo unitario. La abscisa de un punto del círculo es $x=\operatorname{sen} s$, o, equivalentemente, $s=\operatorname{arc\,sen} x$. Como se sabe, $ds=\frac{dx}{\sqrt{1-x^2}}$, o, integrando, $s=\int\frac{dx}{\sqrt{1-x^2}}$. Se desprende de aquí que

$$sds=\frac{dx}{\sqrt{1-x^2}}\int\frac{dx}{\sqrt{1-x^2}}.(1)$$

Integremos ambos miembros desde $x=0$ hasta $x=1$, y puesto que al ir x de 0 a 1, s va de 0 a $\frac{\pi}{2}$, obtenemos del lado izquierdo $\frac{s^2}{2}$ entre 0 y $\frac{\pi}{2}$, es decir, $\frac{\pi^2}{8}$. En el miembro derecho de (1) debemos, en primer lugar, calcular $\int\frac{dx}{\sqrt{1-x^2}}$. Euler lo hizo de la manera que solía: desarrollando el integrando en serie de potencias; por fortuna, en este caso viene en nuestro auxilio el Teorema del Binomio (el que Newton extendió a exponentes fraccionarios). Así pues,

$$(1-x^2)^{-\frac{1}{2}}=1+\frac{1}{2}x^2+\frac{3}{8}x^4+\frac{5}{16}x^6+\frac{35}{128}x^8+\cdots$$

Es preferible para nuestros fines dejar las cuentas indicadas en los coeficientes, así:

$$(1-x^2)^{-\frac{1}{2}}=1+\frac{1}{2}x^2+\frac{1\cdot3}{2\cdot4}x^4+\frac{1\cdot3\cdot5}{2\cdot4\cdot6}x^6+\frac{1\cdot3\cdot5\cdot7}{2\cdot4\cdot6\cdot8}x^8+\cdots$$

Integrando término a término —reserve el lector sus objeciones hasta el siglo diecinueve; recuerde que estamos en 1741— se obtiene, tras multiplicar por el factor restante, $\frac{dx}{\sqrt{1-x^2}}$,

$$\begin{aligned}sds=\frac{xdx}{\sqrt{1-x^2}}+\frac{1}{2\cdot3}\frac{x^3dx}{\sqrt{1-x^2}}+\frac{1\cdot3}{2\cdot4\cdot5}\frac{x^5dx}{\sqrt{1-x^2}}+\\ \frac{1\cdot3\cdot5}{2\cdot4\cdot6\cdot7}\frac{x^7dx}{\sqrt{1-x^2}}+\cdots\end{aligned}$$

Ahora, naturalmente, integramos el miembro derecho de la igualdad término a término, entre 0 y 1. La integración de la serie nos proporcionará una serie numérica cuya suma será entonces $\frac{\pi^2}{8}$, como ya vimos. Empecemos por calcular la integral del primer sumando:

$$I(1)=\int_0^1\frac{xdx}{\sqrt{1-x^2}}=-\sqrt{1-x^2}\Big|_0^1=1.$$

Las integrales de los demás sumandos tienen la forma

$$I(n+2) = \int \frac{x^{n+2}dx}{\sqrt{1-x^2}},$$

con $n \geq 1$. Integrando por partes con $u = x^{n+1}$ y $dv = \frac{xdx}{\sqrt{1-x^2}}$ tendremos

$$\begin{aligned} I(n+2) &= -x^{n+1}\sqrt{1-x^2}\Big|_0^1 \\ &\quad +(n+1)\int_0^1 x^n\sqrt{1-x^2} \\ &= 0+(n+1)\int_0^1 \frac{x^n(1-x^2)}{\sqrt{1-x^2}} \\ &= (n+1)\int \frac{x^n dx}{\sqrt{1-x^2}} - (n+1)I(n+2), \end{aligned}$$

de donde $I(n+2) = \frac{n+1}{n+2}I(n)$. De esta manera tenemos

$$\begin{aligned} I(3) &= \frac{2}{3}I(1) = \frac{2}{3}; I(5) = \frac{4}{5}I(3) = \frac{2\cdot 4}{3\cdot 5}; \\ I(7) &= \frac{6}{7}I(5) = \frac{2\cdot 4\cdot 6}{3\cdot 5\cdot 7}, \end{aligned}$$

etc., de modo que

$$\begin{aligned} \frac{\pi^2}{8} &= 1+\tfrac{1}{2\cdot 3}\tfrac{2}{3}+\tfrac{1\cdot 3}{2\cdot 4\cdot 5}\tfrac{2\cdot 4}{3\cdot 5}+\tfrac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6\cdot 7}\tfrac{2\cdot 4\cdot 6}{3\cdot 5\cdot 7}+\cdots \\ &= 1+\tfrac{1}{3^2}+\tfrac{1}{5^2}+\tfrac{1}{7^2}+\cdots \end{aligned}$$

Prometí mostrar cómo encontró Euler, por segunda vez, la suma que obsesionó a Jakob Bernoulli, y en vez de eso he mostrado cómo encontró otra. Pido un poco de paciencia. Observemos que todo entero n puede escribirse en la forma $n = 2^k \cdot m$, donde m es impar. Por supuesto, si n es impar k será 0. Entonces $n^2 = 2^{2k}\cdot m^2 = 4^k \cdot m^2$, en otras palabras, el cuadrado de cualquier entero —aunque sólo nos interesan los positivos— puede ponerse como el producto de una potencia de 4 y un cuadrado impar. Ahora bien, puede verse que al efectuar el producto $(1+\frac{1}{4}+\frac{1}{4^2}+\frac{1}{4^3}+\cdots)(1+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\cdots)$ se obtiene una serie cuyos términos tienen como numerador 1 y como denominadores todos los posibles productos de una potencia de 4 por un cuadrado impar, es decir, los denominadores son los cuadrados de todos los números naturales: hemos vuelto a Basilea. Puesto que el primer factor es una serie geométrica de razón $\frac{1}{4}$ y por consiguiente, de suma $\frac{4}{3}$, concluimos que

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\cdots = \frac{4}{3}\frac{\pi^2}{8} = \frac{\pi^2}{6}.$$

El dar una segunda o una tercera solución de un mismo problema era característico de Euler. ¿Exhuberancia creativa, pero ingenua, o más bien una sobria estrategia de corroboración de resultados obtenidos mediante recursos no probados? Sin titubear, me inclino a lo segundo. En el presente ejemplo, Euler bien pudo percibir la debilidad de su argumento en el sentido de que el "polinomio"

$$1-\frac{x^2}{3!}+\frac{x^4}{5!}-\frac{x^6}{7!}+\cdots$$

y el "polinomio"

$$(1-\frac{x^2}{\pi^2})(1-\frac{x^2}{4\pi^2})(1-\frac{x^2}{9\pi^2})\cdots$$

son iguales por tener las mismas raíces y el mismo valor en $x = 0$. El primer "polinomio" es, por supuesto, la función $\frac{\operatorname{sen} x}{x}$; Ed Sandifer hace notar que la función $e^x\frac{\operatorname{sen} x}{x}$ también se anula en los múltiplos no nulos de π, y sólo ahí, y vale 1 en $x = 0$, pero es distinta de $\frac{\operatorname{sen} x}{x}$, por lo que no puede compartir con ésta una misma representación como producto infinito. Surge, pues, la necesidad de corroborar el resultado.

La historiografía tradicional nos pinta un Euler de espíritu excepcionalmente vigoroso, pero carente de sutileza, un Atila matemático capaz de inmensas conquistas, pero insensible a los sentimientos de los pueblos sometidos, un Euler, digámoslo ya sin abusar de la metáfora, insensible a la diferencia, que ahora nos parece irreductible, entre las series convergentes y las divergentes [7, p.147]. De aquí sólo hay un paso a insinuar que nuestro homenajeado hizo toda clase de cosas estupendas, pero porque no quiso, o no supo, hacer la única que importaba —crear una teoría "rigurosa" de la convergencia de series— Euler es en realidad un poco menos que matemático. Por no dar sino un ejemplo, significativo porque proviene de un historiador cuidadoso, consideremos esta cita: "La falta de cuidado con que Euler manejaba el infinito es evidente también en su uso de las series divergentes" [6, p. 246]. Euler era descuidado, irresponsable, jugando con el infinito como un niño con cuchillos.

Sin embargo, si examinamos lo que Euler escribió sobre las series divergentes, nos encontramos, por el contrario con un Euler mesurado, que sopesa imparcialmente —o casi— posiciones opuestas, consciente de las dificultades a vencer, un Euler cuidadoso, un Euler responsable.

En primer lugar, Euler distingue perfectamente entre series convergentes y divergentes. Así abre su *De seriebus divergentibus*:

> Si consideramos series convergentes aquéllas cuyos términos decrecen continuamente y a la larga, cuando la serie se prolonga al infinito, desaparecen del todo, se aceptará en el acto que aquéllas cuyos términos no tienden a cero en el infinito, sino que permanecen finitas o crecen al infinito, puesto que no son convergentes, deben asignarse a la clase de las divergentes [7, p.144; 8, p. 205].

Sin duda, nos vemos tentados en este momento a blandir el índice como un estoque, dispuestos a clavarlo en el punto donde Euler nos dice que las series convergentes son precisamente aquéllas cuyo término general tiende a cero, como si ignorara la divergencia de la serie armónica tan bien conocida de su tutor Johann Bernoulli —desde luego, no la ignoraba. Envainemos el índice. No intento demostrar que Euler anticipó a Cauchy, pues no deseo cruzar la delgada línea que separa la historia de la fantasía. Tan sólo señalo que casi siempre estaríamos de acuerdo con Euler cuando llama a tal serie convergente, divergente tal otra, pues aunque su definición puede hacernos creer que consideraba convergente a toda serie cuyo término general tienda a cero, tal no es el caso.

El objetivo de Euler al escribir *De seriebus divergentibus* es zanjar la disputa entre los partidarios de asignar sumas a las series divergentes —entre quienes se contaba Leibniz— y quienes se rehusaban a ello. Llamaré a los primeros sumadores o, para mayor brevedad, *sumas*. En cuanto a los segundos, me haré eco de Euler cuando dice: "Aquéllos que niegan que las sumas que habitualmente se asignan a las series divergentes sean correctas, no sólo no proponen una alternativa, sino que se niegan a imaginar siquiera la suma de una serie divergente" [8, p. 210; 7, p.147]. Euler no es aquí del todo neutral; parece estar a punto de llamar intransigentes a los que se niegan a sumar series divergentes. Los llamaré *intras.*

Divide Euler las series divergentes en cuatro clases, según que su término general tenga un límite finito (distinto de cero, claro está) o infinito, y según sean alternantes o no. Nadie parece haber considerado series con una distribución arbitraria de términos positivos y

negativos antes del siglo diecinueve (pero si a alguien le consta lo contrario, me hará su deudor haciéndomelo saber). Euler, siempre preocupado de hacerse entender, añade dos ejemplos de cada clase:

I	$1+1+1+1+1+1+1+\cdots$
	$\frac{1}{2}+\frac{2}{3}+\frac{3}{4}+\frac{4}{5}+\frac{5}{6}+\frac{6}{7}+\cdots$
II	$1-1+1-1+1-1+\cdots$
	$\frac{1}{2}-\frac{2}{3}+\frac{3}{4}-\frac{4}{5}+\frac{5}{6}-\frac{6}{7}+\cdots$
III	$1+2+3+4+5+6+\cdots$
	$1+2+4+8+16+32+\cdots$
IV	$1-2+3-4+5-6+\cdots$
	$1-2+4-8+16-32+\cdots$

Desde luego, los *intras* no hacían distinciones entre estos cuatro tipos; para ellos no había sino series convergentes y series divergentes. Euler presenta los argumentos de este bando referidos a la serie geométrica en una variable, sin que quede claro si lo hace por razones didácticas, vistiendo con un ropaje concreto argumentos que, sin él, podrían sonar demasiado abstractos a oídos inexpertos, o si todo el debate giraba en torno a series geométricas particulares. He aquí el argumento: El desarrollo

$$\frac{1}{1+a}=1-a+a^2-a^3+a^4-a^5+a^6-\cdots$$

no es válido a menos que $a<1$ [¡ $-1<a<1$! —el lector] [Aprecio la atención con que sigues mi desmadejado discurso, apreciable lector, pero debo aclarar que no se trata de un error mío. Euler escribió: *nisi a sit fractio unitatis minor* [8, p. 207] es decir, "a menos que a sea una fracción menor que la unidad" —el autor]. El argumento continúa así: pues si interrumpimos la división [de 1 entre $1+a$] en un momento cualquiera, obtenemos

$$\frac{1}{1+a}=1-a+a^2-a^3+\cdots\pm a^n-(\pm\frac{a^{n+1}}{1+a}),$$

donde se elige el signo $+$ si n es par y $-$ si n es impar. Sin embargo el residuo $\pm\frac{a^{n+1}}{1+a}$ no puede despreciarse a menos que se reduzca a cero, lo que ocurre sólo en caso de que $a<1$, que es precisamente el caso en que la serie es convergente. Si $a\geq 1$, entonces es necesario tener en cuenta el residuo. No es válido ignorarlo con base en el argumento de que el infinito no es ni par ni impar, por lo cual no puede decidirse el signo del residuo, pues es absurdo pensar que un número entero, incluso si es infinito, carezca de paridad. Puede verse que los *intras* no son los antecesores de Weierstrass.

La réplica de los *sumas* consiste en observar que el infinito es indeterminado, por lo que no puede atribuírsele paridad; además, la idea de prolongar una serie al infinito excluye la idea de un último término tras el cual se coloca el residuo. Es imposible poner el residuo en su lugar. Así pues, el residuo no solo puede, sino que debe ser ignorado.

Los *intras* tienen todavía un as en la manga: las series del tercer tipo, cuyo comportamiento es punto menos que civilizado: vemos que al hacer $x=1$ en la identidad

$$1+2x+3x^2+4x^3+5x^4+\cdots=\frac{1}{(1-x)^2}$$

se obtiene

$$1+2+3+4+5+\cdots=\frac{1}{(1-1)^2}=\infty,$$

que es lo esperado, mientras que al hacer $x=2$ en la identidad

$$1+x+x^2+x^3+x^4+x^5+\cdots=\frac{1}{1-x}$$

resulta

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

que no es lo esperado. De las dos series del tipo III, la segunda, cuyos sumandos, con la única excepción de los dos primeros, son mayores que los de la primera, debiera tener una suma mayor, pero su suma es negativa. Si alguien me lee y me ha dejado llegar hasta aquí, sin exigirme cuentas por mi uso de la palabra *identidad*, merece desde luego una explicación. Newton había mostrado cómo desarrollar funciones algebraicas en serie de potencias simplemente efectuando las operaciones indicadas. Por ejemplo, si en

$$\frac{1}{1-x}$$

dividimos de hecho 1 entre $1-x$, obtendremos

$$1+x+x^2+x^3+x^4+x^5+\cdots$$

De igual manera, al dividir 1 entre

$$(1-x)^2=1-2x+x^2,$$

se obtiene

$$1+2x+3x^2+4x^3+5x^4+\cdots$$

Estos cálculos, al ser realizados mediante símbolos a los que no se han asignado valores específicos, parecen ser válidos para cualquier valor de la variable y ésta era ciertamente la creencia dominante durante el siglo dieciocho.

Pero regresemos a nuestra paradoja: ¡parece requerir que $-1>\infty$! Los *sumas* se verán en aprietos si insisten en asignar a las series divergentes sumas correspondientes a las expresiones cerradas que les dan origen. Pero los *sumas* no disponen de otra opción. Debemos reconocer que los *sumas* no eran pusilánimes, pues lejos de desanimarse agarran el toro por los cuernos: aceptan que $-1<0$ y también que $-1>\infty$, diciendo que hay una clase de cantidades negativas menores que cero, y otra de las que son mayores que infinito; las primeras provienen de *restar* de una cantidad otra mayor, mientras que las segundas se obtienen al *dividir* una cantidad positiva entre una negativa (del primer tipo), como ocurre en

$$1+2+4+8+16+\cdots=\frac{1}{1-2}=\frac{1}{-1}.$$

Se tienen dos clases esencialmente distintas de números negativos y ya no es posible escribir $\frac{1}{-1}=1-2$, o en otras —inquietantes— palabras, algunas reglas ordinarias del álgebra, como la de los signos, quedan suspendidas. Este es un Rubicón que Euler no estaba dispuesto a cruzar, por lo que aquí su camino se separa del de los *sumas*, con quienes lo hemos visto hasta ahora mantener una discreta afinidad. Nunca intervino Euler en una controversia simplemente para tomar partido: su fin fue siempre hacer avanzar la matemática.

Euler tiene una mejor idea que abrogar la regla de los signos: substituir la recta real por una enorme circunferencia real. Así, cuando partiendo de 0 nos movemos a la derecha recorremos números positivos cada vez más grandes, pasaremos en algún momento por

∞, y entraremos entonces, sin cambiar de dirección, en la región de los números negativos. De esta manera vemos que los números negativos se encuentran a la derecha de ∞, es decir, que son mayores que ∞. A la vez, los números negativos están a la izquierda de 0, lo que los hace menores que 0. De esta forma da Euler una elegante, y de ninguna manera absurda, solución al problema planteado por el excesivo entusiasmo de los *sumas*, sin pagar el precio, demasiado alto, de convertir al álgebra en una tierra sin ley.

Pero no para aquí el ingenio creador de Euler. Observa acto seguido que para resolver de manera satisfactoria el problema de asignar sumas a las series divergentes no es necesario resolver previamente el problema del orden en los números reales, ni mucho menos el de decidir qué leyes algebraicas deben sacrificarse en el altar de las series divergentes.

> 110. Digo, pues, que toda la dificultad se esconde en la palabra *suma*. Si, como es común, tomamos como suma de una serie el agregado de todos sus términos tomados todos juntos en acto [por oposición a reunirlos potencialmente], entonces, sin duda alguna, sólo las series convergentes, que continuamente se aproximan más a un cierto valor mientras más términos de hecho se suman, pueden tener sumas. Por otra parte, las series divergentes, cuyos términos no decrecen, ya sea que los signos $+$ y $-$ se alternen o no, no poseen en lo absoluto una suma fija, si por la palabra suma entendemos el agregado de todos sus términos. [...]
>
> 111. Estos inconvenientes y aparentes contradicciones pueden evitarse si atribuimos a la palabra *suma* un significado distinto del usual. Digamos pues que la suma de una serie cualquiera es la expresión finita de cuyo desarrollo surge la serie. En este sentido la suma de la serie $1 + x + x^2 + x^3 + \cdots$ es $\frac{1}{1-x}$, puesto que la serie tiene su origen en el desarrollo de la fracción, no importa qué valor demos a x. Con este acuerdo, si una serie fuere convergente, la nueva definición de la palabra *suma* coincide con la usual; y como las series divergentes no tienen sumas propiamente dichas, no surge ningún inconveniente del significado nuevo del término. Así pues, por medio de esta definición se salvaguarda la utilidad de las series divergentes y es posible reivindicarlas de toda injuria. [9, p.61; 10, p.78-9].

Es así como generalizamos un concepto matemático: incluyendo en él nuevos objetos, pero cuidando que conserve su significado original cuando lo restringimos a los objetos familiares. La actitud que muestra aquí Euler es típica: se resiste a tomar partido por una posición que restrinja a la matemática, como lo es en este caso la de los *intras*. La misma actitud toma ante dÁlembert en la controversia que sostuvo con él durante casi cuatro décadas acerca de las vibraciones de una cuerda. El problema consiste en determinar el movimiento de una cuerda tensa, fija en sus extremos, cuando se la suelta tras de obligarla a adoptar una forma cualquiera. DÁlembert encuentra una solución que no se aplica a cualquier forma inicial de la cuerda. DÁlembert acepta la restricción a la que su razonamiento lo ha llevado y concluye que en los demás casos, es decir, cuando a la cuerda se le da una forma que no satisface las restricciones, la cuerda desde luego vibra de algún modo, pero el Análisis es impotente para describir su movimiento. La respuesta de Euler aparece en el siguiente volumen de la *Histoire de lÁcademie Royale de Berlin*, y tiene como fin poner en términos más claros que los de dÁlembert la deducción de la ecuación diferencial satisfecha por los posibles movimientos de la cuerda, pero sobre todo eliminar la restricción que dÁlembert creía necesario imponer a la solución [11, p. 23-4].

Dejemos la controversia de la cuerda vibrante, pues Euler es partícipe en ella desde su inicio, para narrar su intervención en otra controversia: la que se dió entre Leibniz y Johann Bernoulli acerca de los logaritmos de los números negativos e imaginarios. Aquí, como en el debate entre los *sumas* y los *intras,* Euler interviene sólo como árbitro. Aunque —según estimación de Eneström— Euler escribió su *De la controverse entre Mrs. Leibniz et Bernoulli sur les logarithmes des nombres negatifs et imaginaires* en 1747, lo presentó hasta 1749 (se publicó en 1751). Johann Bernoulli había muerto el primer día de 1748. Es comprensible que Euler haya pospuesto la presentación pública de su juicio sobre la controversia, dado que Euler no falla a favor de su antiguo mentor y amigo. Por otra parte, Euler escribió una versión más breve de su análisis de la controversia, *Sur les logarithmes des nombres negatifs et imaginaires*, que no se publicó sino hasta 1862, pero que según C. G. J. Jacobi, fue presentada a la Academia el 7 de septiembre de 1747.

El debate entre Leibniz y Johann Bernoulli se centra en los logaritmos de números negativos: mientras que Leibniz afirmaba que eran imaginarios, Bernoulli creía no sólo que eran reales, sino de hecho iguales a los de sus valores absolutos es decir que, modernizando la notación, $\ln(-a) = \ln(a)$. Presentaré el debate como lo presenta Euler, con varios argumentos a favor de la posición de cada uno, objeciones de cada uno a la posición del otro, objeciones del propio Euler a dichas objeciones y sus juicios sobre el peso de todos los argumentos presentados a favor o en contra, y finalmente la solución del propio Euler al problema y la explicación de como da cuenta de todas las dificultades. Me esforzaré por ser breve, pero sin dejar de dar una idea de un estilo de escribir matemáticas que se ha perdido y no por falta de encanto.

Creo, además, que refleja la personalidad de nuestro homenajeado mejor que un par de anécdotas. Debo anotar, antes de seguir, que no siempre es claro cuando Euler reproduce los argumentos de Bernoulli y los de Leibniz y cuando los mejora, o incluso proporciona los propios para llenar algún hueco dejado por los contrincantes. Euler hace claramente un esfuerzo por dar a cada posición la mayor fuerza posible, y ello no sólo por enfatizar que el hecho mismo de que haya un desacuerdo entre dos grandes matemáticos en una cuestión de matemática pura es anómalo y no debe tomarse a la ligera. Es muy probable que Euler tuviese interés en mostrar la honestidad intelectual de los contrincantes, dejando que la fuerza misma de las objeciones de que cada postura era susceptible mostrara que el aferrarse cada quien a la suya no nacía de motivos frívolos. Atribuye Euler a Bernoulli cuatro argumentos con los que "fortalece su opinión". El primero es que

$$d\ln(-x) = \frac{-dx}{-x} = \frac{dx}{x} = d\ln(x),$$

es decir $\ln(-x)$ y $\ln(x)$ tienen la misma diferencial, de donde concluye que deben ser iguales.

Una segunda razón esgrimida por Bernoulli en defensa de su tesis es que la curva *logarítmica* (nosotros la llamamos exponencial) satisface la ecuación $dx = \frac{dy}{y}$, o bien $ydx = dy$; vemos que si se cambia y por $-y$ en esta ecuación, la ecuación subsiste. Esto prueba, en opinión de J. Bernoulli, que la curva es simétrica respecto al eje x. De ello se sigue que a las ordenadas y y $-y$ corresponde una misma abscisa x, pero la relación entre abscisas y ordenadas en esta curva es $x = \ln y$, luego $\ln y = \ln(-y)$.

La tercera razón que da Bernoulli es que todas las curvas que satisfacen $dx = \frac{dy}{y^n}$ para n impar son simétricas respecto al eje x, luego lo mismo debe ser cierto para $n = 1$.

La cuarta es, que puesto que $\ln(x^n) = n\ln x$, para $n = 2$ se tiene

$$\ln(-a)^2 = 2\ln(-a),$$

por otra parte, $(-a)^2 = a^2$, por lo que

$$\ln(-a)^2 = \ln(a^2) = 2\ln a,$$

de donde $2\ln a = 2\ln(-a), \ln a = \ln(-a)$. Euler considera este argumento como el más sólido de los presentados por Bernoulli. En cuanto a los dos primeros, un estudiante de cálculo alerta no podrá evitar exclamar:
«¡la constante de integración!». Euler señala, en efecto, que

$$d\ln(mx) = \frac{mdx}{mx} = \frac{dx}{x} = d\ln x,$$

de modo que si el argumento de Bernoulli fuese válido, se concluiría que $lmx = lx$ para cualquier valor de m, cosa que sin duda rechazaría el propio Bernoulli. Acto seguido observa que de la igualdad de las diferenciales de dos funciones sólo puede concluirse que difieren en una constante, no que son iguales. Resulta curioso que no viese esto el propio Bernoulli, y debemos abstenernos de inferir que se trata de ignorancia o descuido de su parte. Hay seguramente detrás de ello alguna concepción que identifica una curva con su ecuación, diferencial o no. Por otra parte, Euler va demasiado lejos al decir que el hecho de que las curvas $x = \ln(my)$ y $x = \ln y$ satisfacen ambas la ecuación $ydx = dy$ muestra que no "se puede juzgar la forma de una curva considerando sólo su ecuación diferencial " [12, p. 145].

Al primer argumento de Bernoulli ($d\ln x = d\ln(-x)$, etc.), Leibniz había respondido que no puede escribirse esta igualdad, porque sólo uno de los miembros tiene sentido: la regla para la diferencial del logaritmo sólo es válida para $x > 0$, nos dice Leibniz. Para nuestros fines resulta más interesante la objeción que Euler hace a esta respuesta:

> Es de todo punto necesario reconocer que esta objeción es no solamente extremadamente débil, puesto que no la sustenta ninguna razón válida, sino que echaría por tierra todo el cálculo diferencial de logaritmos. Puesto que dicho cálculo versa sobre cantidades variables, es decir, sobre cantidades bajo un punto de vista general, si la igualdad $d\ln x = \frac{dx}{x}$ no fuera válida en general, sea cual fuere el valor que se le de a x, sea positivo o negativo, o incluso imaginario, no podría hacerse uso de la regla en cuestión, pues la validez del cálculo diferencial se asienta en la generalidad de las reglas que lo constituyen [12, p. 143]

He aquí una profesión de fe reveladora. Esta apasionada confianza en la generalidad de las reglas del cálculo, en la generalidad como ingrediente básico de los fundamentos del cálculo, la profesa Euler en un contexto particularmente significativo: en un artículo sobre una dificultad que surge de problemas conceptuales en el seno del cálculo. Debe estar seguro de que su punto de vista será bien recibido, pues aspira a dejar zanjada la controversia. No es sino hasta el *Cours dÁnalyse* de Cauchy que encontramos que "el rigor que se exige en geometría" se contrapone a "las razones extraídas de la generalidad del álgebra" [13, p. ii].

Pasemos a las razones que Euler presenta en nombre de Leibniz. Consideremos en primer término el desarrollo

$$\ln(1+x) = x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \frac{1}{4}x^4 + \frac{1}{5}x^5 - \frac{1}{6}x^6 + \cdots$$

Si hacemos $x = 0$, tendremos $\ln 1 = 0$. Para obtener $\ln(-1)$ debemos tomar $x = -2$, con lo cual obtenemos

$$\ln(-1) = -2 - \frac{1}{2}\cdot 4 - \frac{1}{3}\cdot 8 - \frac{1}{4}\cdot 16 - \frac{1}{5}\cdot 32 - \frac{1}{6}\cdot 64 - \cdots$$

Esta suma es claramente distinta de 0, es decir, $\ln(-1)$ no es cero como lo requiere la tesis de Johann Bernoulli.

La siguiente razón que Euler atribuye a Leibniz consiste en observar que si $y = \ln x$, entonces $x = e^y$, donde e es "el número cuyo logaritmo es 1, que, como se sabe, vale aproximadamente $e = 2{,}718281828459$; siendo entonces y el exponente de la potencia de e que es igual al número x, es claro que ningún exponente real de una potencia de e podrá producir un número negativo". Puesto que, según testimonio de Boyer, la *Introductio* de Euler "contiene el primer tratamiento algorítmico de los logaritmos como exponentes" [14, p. 73], nos es permitido sospechar que este argumento representa una cortesía de Euler hacia Leibniz.

También empleando el desarrollo en serie de la función exponencial,

$$e^y = 1 + \frac{y}{1} + \frac{y^2}{1\cdot 2} + \frac{y^3}{1\cdot 2\cdot 3} + \frac{y^4}{1\cdot 2\cdot 3\cdot 4} + \cdots,$$

"que es siempre convergente, ..., de modo que las objeciones basadas en la naturaleza de las series convergentes no tienen lugar aquí" [12, p. 150] puede llegarse a la conclusión de que $\ln(-1)$ no es 0. En efecto, si y es el logaritmo de x, tendremos

$$x = 1 + \frac{y}{1} + \frac{y^2}{1\cdot 2} + \frac{y^3}{1\cdot 2\cdot 3} + \frac{y^4}{1\cdot 2\cdot 3\cdot 4} + \cdots$$

y, si y es el logaritmo de -1, es decir, si $x = -1$, se tiene

$$-1 = 1 + \frac{y}{1} + \frac{y^2}{1\cdot 2} + \frac{y^3}{1\cdot 2\cdot 3} + \frac{y^4}{1\cdot 2\cdot 3\cdot 4} + \cdots,$$

de donde resulta que y no puede ser 0, porque de ello se seguiría $-1 = 1$.

Presenta Euler enseguida la réplica —no la atribuye específicamente a Bernoulli— a los argumentos precedentes. En el caso del primero, volvemos al terreno de las series divergentes. ¿Porqué no podría ser, a fin de cuentas, $-2 - \frac{1}{2}\cdot 4 - \frac{1}{3}\cdot 8 - \frac{1}{4}\cdot 16 - \frac{1}{5}\cdot 32 - \frac{1}{6}\cdot 64 - \cdots = 0$? De la serie geométrica

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + x^4 - x^5 + x^6 - \cdots$$

se obtiene en el caso en que $x = -2$ la serie

$$-1 = 1 + 2 + 4 + 8 + 16 + \cdots$$

y en el caso $x = -3$ la serie

$$-\frac{1}{2} = 1 + 3 + 9 + 27 + 81 + \cdots$$

y sumas cada vez más cercanas a 0 mientras más grande en valor absoluto sea x, conservándose negativa. De hecho, si a esta última serie sumamos la serie

$$\frac{1}{2} = 1 - 1 + 1 - 1 + 1 - \cdots$$

término a término, obtenemos

$$0 = 2 + 2 + 10 + 26 + 82 + \cdots$$

"Así pues, si la suma de esta serie es 0, ¿por qué sería absurdo mantener que

$$-2 - \frac{1}{2}\cdot 4 - \frac{1}{3}\cdot 8 - \frac{1}{4}\cdot 16 - \frac{1}{5}\cdot 32 - \frac{1}{6}\cdot 64 - \cdots = 0?$$

Por lo tanto la primera razón no es convincente".[12, p.151]. Queda claro que el haber extendido el significado de la palabra *suma* tiene consecuencias.

La segunda razón, que nos parece más sólida que la primera, también puede ponerse en tela de juicio, ya que si $x = e^y$, donde y es el logaritmo de x, cuando y es una fracción de denominador par "debemos reconocer que el valor de e^y, y por lo tanto el de x, es tanto negativo como afirmativo"[*ibid.]*

Puede añadirse que si $\ln(-1)$ fuese imaginario, como lo pretende Leibniz, entonces su doble, es decir, el logaritmo de $(-1)^2 = +1$ tendría que serlo también, cosa que contradice el principio básico $\ln 1 = 0$. Por otra parte, si lo correcto es $\ln(-1) = \ln 1 = 0$, como lo quiere Bernoulli, entonces $\ln\sqrt{-1} = \frac{1}{2}\ln(-1) = 0$. Desafortunadamente, este resultado contradice uno del propio Bernoulli, quien había encontrado que $\ln\sqrt{-1} = \frac{1}{2}\pi\sqrt{-1}$, probablemente mediante alguna manipulación formal parecida a la siguiente:

Sabemos que

$$\int_0^1 \frac{dx}{\sqrt{1-x^2}} = \arcsin x|_0^1 = \frac{\pi}{2}.$$

Haciendo el cambio de variable $x = \sqrt{-1}z$ tenemos que

$$\begin{aligned}\frac{\pi}{2} &= \int_0^1 \frac{dx}{\sqrt{1-x^2}} = \sqrt{-1}\int_0^{-\sqrt{-1}} \frac{dz}{\sqrt{1+z^2}} \\ &= \sqrt{-1}\ln(z+\sqrt{1+z^2})|_0^{-\sqrt{-1}} \\ &= \sqrt{-1}\ln(-\sqrt{-1}) = \sqrt{-1}\ln(\frac{1}{\sqrt{-1}}) \\ &= -\sqrt{-1}\ln\sqrt{-1},\end{aligned}$$

de donde se sigue la igualdad citada.

Sin duda el lector, está al borde de un ataque de nervios. O de vértigo. O de impaciencia por saber qué hilo de Ariadna nos tenderá Euler para extraernos de este laberinto de contradicciones. La simplicidad del que nos tiende revela el genio de su autor:

> Cuando se dice que el logaritmo de un número dado es el exponente de aquélla potencia de cierto número arbitrariamente escogido, la cual coincide con el número elegido, nada parece faltar a la verdad de la aseveración. Bien cierto es que nada falta, pero comúnmente se acompaña esta idea de otra que no le va bien: y es que de ordinario se asume, sin tomar conciencia de ello, que a cada número no le corresponde sino un logaritmo; mas por poco que se reflexione en ello, habrá de verse que todas dificultades y contradicciones que parecían sumergir en la perplejidad a la doctrina de los logaritmos no persisten que en tanto se da por sentado que a cada número le corresponde un único logaritmo [12, pp. 155-6].

Procede a continuación Euler a demostrar que cada número posee una infinidad de logaritmos. Haré algunos cambios de inspiración euleriana en la prueba de Euler. Comenzaré por considerar la expresión $(1+\frac{1}{M})^M$, donde, como Euler lo hizo, tomamos M infinito; (el análisis no estándar iniciado por Abraham Robinson en 1960 reivindica el uso de números infinitos, ver [15]; quien prefiera el análisis estándar, es decir, el usual, al no estándar, puede consultar [16, capítulo 4]). Se trata de elevar un binomio a cierta potencia; hagámoslo:

$$\begin{aligned}(1+\frac{1}{M})^M &= 1 + M(\frac{1}{M}) + \frac{M(M-1)}{2!}(\frac{1}{M})^2 \\ &\quad + \frac{M(M-1)(M-2)}{3!}(\frac{1}{M})^3 \\ &\quad + \frac{M(M-1)(M-2)(M-3)}{4!}(\frac{1}{M})^4 \\ &\quad + \cdots \\ &= 1 + 1 + (1-\frac{1}{M})\frac{1}{2!} \\ &\quad + (1-\frac{1}{M})(1-\frac{2}{M})\frac{1}{3!} \\ &\quad + (1-\frac{1}{M})(1-\frac{2}{M})(1-\frac{3}{M})\frac{1}{4!} \\ &\quad + \cdots\end{aligned}$$

Puesto que M es un número infinito, cometemos un error infinitamente pequeño al tomar $1-\frac{k}{M} = 1$ para cualquier k finita. Podemos entonces escribir

$$(1+\frac{1}{M})^M = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \cdots,$$

que vale aproximadamente $2{,}718281828459$ y que llamaré, ¿por qué no?, e.

Evaluemos ahora la expresión $(1+\frac{y}{N})^N$, para y finita y N infinita; para ello, tomemos $M = \frac{N}{y}$: ciertamente M será infinita. Entonces

$$(1+\frac{y}{N})^N = (1+\frac{y}{My})^{My} = \left[\left(1+\frac{1}{M}\right)^M\right]^y = e^y.$$

Si $x = e^y$, será $y = \ln x$. Por otra parte, si de $x = (1+\frac{y}{N})^N$ despejamos y, tendremos $\ln x = y = N(x^{\frac{1}{N}} - 1)$. Ahora bien, "como es cosa segura que $x^{\frac{1}{2}}$ posee dos valores, $x^{\frac{1}{3}}$ tres, $x^{\frac{1}{4}}$ cuatro. y así sucesivamente, será igualmente seguro que $x^{\frac{1}{N}}$ posee una infinidad de valores, puesto que N es infinita, ... por lo que el número x deberá tener una infinidad de logaritmos" [12, p. 157].

De la infinidad de logaritmos de 1, sólo el 0 es real; resulta ahora claro que de la igualdad $2\ln(-1) = \ln 1$ no se concluye necesariamente que $\ln(-1) = 0$, sino únicamente que al duplicar los logaritmos de -1 los resultados se encuentran entre los logaritmos imaginarios de 1. Mostraré explícitamente esto más adelante. De la misma manera, $4\ln\sqrt{-1} = \ln 1$ significa que al multiplicar por 4 cada logaritmo de $\sqrt{-1}$ se obtiene un logaritmo de 1. Esto se verá aún más claro si determinamos todos los logaritmos de un número dado. Empecemos por hallar todos los logaritmos de un número positivo a. Llamemos A al logaritmo real de a; entonces, puesto que $a = a \cdot 1$, se debe tener $\ln a = \ln 1 + A$, lo que muestra que basta encontrar los logaritmos de 1 para conocer todos los de un número positivo cualquiera.

Como vimos un poco más arriba, si $x = 1$, su logaritmo y satisface $1 = (1+\frac{y}{N})^N$, o bien $(1+\frac{y}{N})^N - 1 = 0$. Por supuesto, $y = 0$ satisface esta ecuación; se trata ahora de encontrar sus raíces complejas. En *Introductio,* vol. I, cap. IX, Euler muestra de manera simple que $p^n - q^n$ puede descomponerse en factores cuadráticos de la forma

$$p^2 - 2pq\cos\frac{2k\pi}{n} + q^2,$$

donde k es un entero. Si resolvemos ahora la ecuación

$$p^2 - 2pq\cos\frac{2k\pi}{n} + q^2 = 0$$

veremos que sus raíces y, por lo tanto las de la ecuación $p^n - q^n = 0$, son

$$p = q\left(\cos\frac{2k\pi}{n} \pm \sqrt{-1}\,\mathrm{sen}\,\frac{2k\pi}{n}\right).$$

Como en nuestro caso $n = N, p = 1 + \frac{y}{N}, q = 1$, obtenemos

$$1 + \frac{y}{N} = \cos\frac{2k\pi}{N} \pm \sqrt{-1}\,\mathrm{sen}\,\frac{2k\pi}{N}.$$

Puesto que N es infinito, $\frac{2k\pi}{N}$ es infinitamente pequeño y por este motivo tenemos que $\cos\frac{2k\pi}{N} = 1$ y que $\mathrm{sen}\,\frac{2k\pi}{N} = \frac{2k\pi}{N}$, de modo que, finalmente,

$$y = \ln 1 = \pm 2\pi k\sqrt{-1}.$$

Quedan así determinados todos los logaritmos de un número positivo cualquiera, a saber, $\ln a = A \pm 2\pi k\sqrt{-1}$, k entero y donde A es el único logaritmo real de a.

Análogamente, para encontrar todos los logaritmos de un número negativo basta determinar los de -1, lo que nos conduce a factorizar la expresión $(1+\frac{y}{N})^N + 1$. Se trata ahora de factorizar una expresión de la forma $p^n + q^n$, cuyos factores cuadráticos son de la forma

$$p^2 - 2pq\cos\frac{(2k-1)\pi}{n} + q^2$$

(*c.f. Introductio* I, IX). Las raíces de estos factores son

$$p = q\left(\cos\frac{(2k-1)\pi}{n} \pm \sqrt{-1}\,\mathrm{sen}\,\frac{(2k-1)\pi}{n}\right).$$

Nuevamente $n = N, p = 1 + \frac{y}{N}, q = 1$, con N infinito, con lo cual se obtiene

$$y = \pm(2k-1)\pi\sqrt{-1};$$

entonces $l - a = A \pm (2k-1)\pi\sqrt{-1}$.

Comparemos los logaritmos de 1 con los de -1:

$$\ln 1 = 0; \pm 2\pi\sqrt{-1}; \pm 4\pi\sqrt{-1}; \pm 6\pi\sqrt{-1}; etc$$

$$\ln(-1) = \pm\pi\sqrt{-1}; \pm 3\pi\sqrt{-1}; \pm 5\pi\sqrt{-1}; \pm 7\pi\sqrt{-1}; etc$$

Ahora es claro lo que señalé antes (escribo en primera persona, pero no soy sino un vocero de Euler), a saber, que si duplicamos los logaritmos de -1 obtenemos exclusivamente logaritmos de 1 (aunque no todos).

En este punto es claro ya como todas las aparentes paradojas que encontramos se desvanecen como gotas de rocío ante el sol veraniego: la fuente de todas ellas es **la creencia tácita en que cada número tiene un único logaritmo**.

Sólo resta encontrar los logaritmos de números complejos. Empieza Euler por mostrar que todo número complejo $a + b\sqrt{-1}$ puede escribirse en la forma

$$c(\cos\theta + \sqrt{-1}\,\mathrm{sen}\,\theta),$$

de lo cual se sigue que

$$\ln(a + b\sqrt{-1}) = C + \ln(\cos\theta + \sqrt{-1}\,\mathrm{sen}\,\theta),$$

donde C es el logaritmo real de c (c es positivo). Para hallar los logaritmos de $\cos\theta + \sqrt{-1}\,\mathrm{sen}\,\theta$, comencemos por observar que

$$\cos\theta + \sqrt{-1}\,\mathrm{sen}\,\theta = \left(1 + \frac{\theta\sqrt{-1}}{N}\right)^N,$$

con N infinito, ya que al desarrollar el binomio se obtiene

$$\begin{aligned}\left(1 + \frac{\theta\sqrt{-1}}{N}\right)^N &= 1 + \frac{\theta\sqrt{-1}}{1} - \frac{\theta^2}{1\cdot 2} - \frac{\theta^3\sqrt{-1}}{1\cdot 2\cdot 3} \\ &+ \frac{\theta^4}{1\cdot 2\cdot 3\cdot 4} + \frac{\theta^5\sqrt{-1}}{1\cdot 2\cdot 3\cdot 4\cdot 5} - \cdots.\end{aligned}$$

Comparando este desarrollo con los desarrollos en serie del seno y el coseno en torno a $x = 0$, se concluye la igualdad propuesta. Procediendo ahora de la misma forma que encontramos los logaritmos de 1, es decir, factorizando la expresión $p^N - q^N$ con $p = 1 + \frac{y}{N}$ y $q = 1 + \frac{\theta\sqrt{-1}}{N}$, se tendrá

$$\begin{aligned}1 + \frac{y}{N} &= \left(1 + \frac{\theta\sqrt{-1}}{N}\right)\left(\cos\frac{2k\pi}{N} \pm \sqrt{-1}\,\mathrm{sen}\,\frac{2k\pi}{N}\right) \\ &= \left(1 + \frac{\theta\sqrt{-1}}{N}\right)\left(1 \pm \frac{2k\pi}{N}\sqrt{-1}\right),\end{aligned}$$

por ser N infinito. Este último producto se reduce a

$$1 + \frac{(\theta \pm 2k\pi)}{N}\sqrt{-1},$$

pues el término con denominador N^2 es despreciable comparado con los de denominador N; de aquí que

$$y = \ln(\cos\theta + \sqrt{-1}\,\mathrm{sen}\,\theta) = (\theta \pm 2k\pi)\sqrt{-1},$$

donde k un entero cualquiera. Por ejemplo, si $\theta = \frac{\pi}{2}$,

$$\cos\theta + \sqrt{-1}\sin\theta = \sqrt{-1}$$

y $\ln\sqrt{-1} = \left(\frac{1}{2} + p\right)\pi\sqrt{-1}$, donde p es un entero par. Nuevamente vemos que al duplicar cada logaritmo de $\sqrt{-1}$ se obtiene siempre un logaritmo de -1, aunque, desde luego, no se obtiene la totalidad de éstos, ya que $2\left(\frac{1}{2} + p\right) = 2p + 1$ es un impar de la forma $4m + 1$, nunca de la forma $4m + 3$. Sin embargo, si observamos que la suma de un logaritmo de $\sqrt{-1}$ con otro debe darnos un logaritmo del producto $\sqrt{-1}\sqrt{-1}$, es decir, un logaritmo de -1, caemos en cuenta de que la suma relevante no es $\left(\frac{1}{2} + p\right) + \left(\frac{1}{2} + p\right)$, sino $\left(\frac{1}{2} + p\right) + \left(\frac{1}{2} + q\right)$, donde p y q son enteros pares arbitrarios; esta última suma sí representa un impar arbitrario, de modo que así sí se obtienen todos los logaritmos de -1.

El artículo de Euler contiene varios otros ejemplos que hacen palpable el hecho de que todas las dificultades de la doctrina de los logaritmos han sido allanadas. El número de tales ejemplos sugiere que Euler está consciente de la necesidad de vencer no sólo las dificultades lógicas, sino también las psicológicas para finiquitar la controversia.

Antes de concluir, quiero hacer notar que la igualdad

$$\cos\theta + \sqrt{-1}\,\mathrm{sen}\,\theta = \left(1 + \frac{\theta\sqrt{-1}}{N}\right)^N,$$

empleada poco ha, y obtenida a partir de los desarrollos en serie del seno y el coseno, es equivalente a la célebre **fórmula de Euler**

$$e^{\theta\sqrt{-1}} = \cos\theta + \sqrt{-1}\,\mathrm{sen}\,\theta,$$

pues como ya Euler nos hizo ver más arriba, $e^{\theta\sqrt{-1}} = \left(1 + \frac{\theta\sqrt{-1}}{N}\right)^N$.

Euler obtuvo esta fórmula, como muchas otras, de más de una manera. Presento una que no involucra series, justo la que exploté

antes con el fin de presentar una posible manera de llegar al resultado de Bernoulli, $\ln\sqrt{-1} = \frac{1}{2}\pi\sqrt{-1}$. Si $y = \operatorname{sen} x$, entonces

$$\begin{aligned} x &= \operatorname{arc\,sen} y = \int \frac{dy}{\sqrt{1-y^2}} = \sqrt{-1}\int \frac{dz}{\sqrt{1+z^2}} \\ &= \sqrt{-1}\ln\left(z+\sqrt{1+z^2}\right), \end{aligned}$$

si hacemos $y = \sqrt{-1}z$. Equivalentemente,

$$\frac{x}{\sqrt{-1}} = \ln\left(\frac{y}{\sqrt{-1}} + \sqrt{1-y^2}\right),$$

es decir,

$$-\sqrt{-1}x = \ln\left(-\sqrt{-1}y + \sqrt{1-y^2}\right)$$

o, lo que es lo mismo,

$$-\sqrt{-1}x = \ln\left(-\sqrt{-1}\operatorname{sen} x + \cos x\right).$$

De aquí obtenemos

$$\begin{aligned} \sqrt{-1}x &= -\ln\left(-\sqrt{-1}\operatorname{sen} x + \cos x\right) \\ &= \ln\left(-\sqrt{-1}\operatorname{sen} x + \cos x\right)^{-1} \\ &= \ln\left(\cos x + \sqrt{-1}\operatorname{sen} x\right). \end{aligned}$$

Basta ahora exponenciar.

Pronto debemos separarnos, pero no te dejaré partir, caro lector, sin antes someterte a una pequeña reflexión sobre el espíritu de nuestro Euler —digo **nuestro** pues seguro estoy de que, como yo, lo amas—. En esta mi humilde pero sentida perorata lo has visto deducir una misma fórmula de varias maneras e intervenir en disputas para adjudicarlas de manera juiciosa. Ambas cosas ocurren en lo que en su momento era la frontera del análisis y ambas son expresión del deseo de Euler de encontrar soluciones sensatas a problemas en cierto sentido urgentes, aún cuando la fundamentación rigurosa de las soluciones halladas estuviese por construirse.

Vemos allí el espíritu de Euler en acción: justo, pero firme en el propósito de hacer crecer la matemática; generoso con sus colegas, incluso con sus adversarios, pero poco dispuesto a aceptar posturas que restrinjan el desarrollo de su amada disciplina o sacrifiquen un resultado bello, más inclinado a abonar que a podar la planta.

Agradezco al Dr. Antonio Rivera Figueroa su gentil invitación a contribuir a la Carta Informativa de la Sociedad Matemática Mexicana.

Referencias

Quien se interese en Euler cuenta con un tremendo recurso: *The Euler Archive*, `http://math.dartmouth.edu/~euler/`. Se encuentran ahí alrededor del 95 % de las publicaciones originales de Euler, en numerosos casos acompañadas de traducciones al inglés. Hay además referencias a publicaciones relativas a Euler y ligas a páginas de interés. Cada artículo de Euler puede localizarse ahí de varias maneras: por tema, por fecha, por publicación en la que apareció originalmente, y por su número en el **Indice de Eneström**, que *The Euler Archive* llama Index Number. Por ser esta última la forma más cómoda de localizar un artículo, es la que daré aquí. Nota: La *Introductio in analysin infinitorum*, volumen 1 corresponde a **E101**. Existe traducción inglesa de ambos volumenes: Euler, *Introduction to Analysis of the Infinite*, Book I (1988) y Book II (1990), ambos traducidos por John D. Blanton y publicados por Springer-Verlag, New York. Puede encontrarse una traducción francesa, que parece más fiel al original latino en *Gallica* (ver [13]). El volumen I se encuentra en `http://gallica.bnf.fr/ark:/12148/bpt6k3884z`; y el volumen II en: `http://gallica.bnf.fr/ark:/12148/bpt6k38858`.

[1] Truesdell, Clifford, "Leonard Euler, Supreme Geometer" en Euler, *Elements of Algebra*, Springer-Verlag, New York, 1984. Se trata de una reimpresión de la quinta edición de la traducción de John Hewlett, publicada en Londres en 1840.

[2] Eulogy of Leonhard Euler by Nicholas Fuss, translated by John S. D. Glaus. Puede encontrarse en *The Euler Archive*, bajo el rubro `Historical Information > The Life of Euler`.

[3] Eulogy of Mr. Euler by the Marquis de Condorcet, translated by John S. D. Glaus. (Véase [2]).

[4] Dunham, William, *Euler, el maestro de todos los matemáticos*, con prólogo y comentarios de Antonio Pérez Sanz. Serie: La matemática en sus personajes, 6. Editorial Nivola, Madrid, 2000. Es traducción de *Euler, the Master of Us All*. The Mathematical Association of America. Dolciani Mathematical Expositions N^{o} 22, Washington, DC., 1999. Este libro es una excelente introducción a la matemática de Euler.

[5] Sandifer, Ed, "Basel Problem with Integrals", que puede encontrarse en la excelente página Ed Sandifer's How Euler Did It, que se encuentra en la página de la Mathematical Association of America (`http://www.maa.org/news/howeulerdidit.html`).

[6] Boyer, Carl B., *The History of the Calculus and Its Conceptual Development*. Dover Publications, Inc., New York, 1959.

[7] Barbeau E.J., Leah, P. J., "Euler's 1760 paper on divergent series," *Historia Mathematica*, 3(1976), 141-160. Este artículo contiene una traducción parcial del *De seriebus divergentibus*. Usé esta traducción, pero la modifiqué en ocasiones por razones de fidelidad al original o de mayor apego a nuestra lengua. Este es el motivo de incluír la referencia [8].

[8] Euler, Leonhard, *De seriebus divergentibus* (**E247**), 1760.

[9] Euler, Leonhard, *Foundations of Differential Calculus*. Translated by John D. Blanton. Springer, New York, 2000. Contiene la traducción de los primeros nueve capítulos de las *Institutiones calculi differentialis cum eius usu in analysi finitorum ac doctrina serierum*, texto que Euler publicó en 1755.

[10] Euler, Leonhard, *Institutiones calculi differentialis cum eius usu in analysi finitorum ac doctrina serierum*, (**E212**), 1755.

[11] Bottazinni, Umberto, *The Higher Calculus: A History of Real and Complex Analysis from Euler to Weierstrass*. Springer-Verlag, New York, 1986.

[12] Euler, *Leonhard, De la controverse entre Mrs. Leibniz et Bernoulli sur les logarithmes des nombres negatifs et imaginaires* (**E168**), 1751.

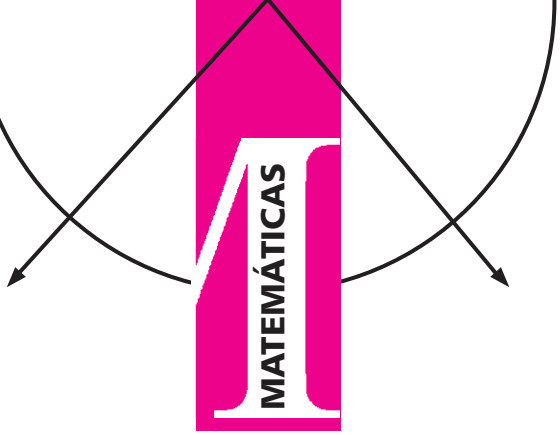
[13] Cauchy, Augustin-Louis, *Cours dÁnalyse de lÉcole Royale Polytechnique. Analyse Algébrique*. Puede encontrarse en la página Web Gallica, bibliothèque numérique de la Bibliothèque Nationale de France, en `http://gallica.bnf.fr/ark:/12148/bpt6k90195m`.

[14] Boyer, Carl B. "The Foremost Textbook of Modern Times". en: Dunham, William, editor, *The Genius of Euler. Reflections on His Life and Work*. The MAA Tercentenary Celebration, volume 2. The Mathematical Association of America, Washington, DC, 2007, pp. 69-74.

[15] Van Osdol, Donovan H., "Truth with respect to an ultrafilter, or how to make intuition rigorous", *American Mathematical Monthly*, **79**, (1972), pp. 355-363.

[16] Rivera Figueroa, Antonio, *Cálculo y sus Fundamentos para Ciencias e Ingeniería*. Editorial Grupo Patria Cultural, México. Por aparecer.

Primo y/o irreducible



Mario Pineda Ruelas
mpr@xanum.uam.mx
UAM-Iztapalapa

1. Introducción

De las estructuras algebraicas más importantes en toda la matemática destaca sin duda el anillo de los números enteros $\mathbb{Z}$. Razones puede haber muchas. Por ejemplo, $\mathbb{Z}$ aparece desde el inicio de nuestra instrucción escolar, aparece en los primeros cursos de la licenciatura y en varias disciplinas de la matemática y, más sentimentalmente, porque es el prototipo de anillo al cual pretendieron parecerse infructuosamente otros anillos. Justamente una de las características más sobresalientes de $\mathbb{Z}$ es la de tener la posibilidad de factorizar en forma única cualquier entero (excepto por supuesto $0, 1$ y -1). Aunque teóricamente sabemos que es posible factorizar, hoy día no podemos hacerlo eficientemente. Esta es una de las claves del éxito de la criptografía. Trabajos de investigación de frontera enfrentan este problema y los avances en cómputo han revelado la necesidad de la interacción entre la teoría de números y la computación. En anillos conmutativos en general no siempre se tiene la propiedad de la factorización única. Así, por medio de algunos ejemplos descubriremos en esta nota a qué se debe este *defecto*. Estrictamente tendremos dos conceptos a la mano: elemento primo y elemento irreducible. ¿Y para qué queremos la factorización única?: pues, entre otras cosas, para resolver algunas ecuaciones diofantinas. El viejo dicho reza: *divide y vencerás*. Como no siempre podemos dividir en un anillo, mejor diremos *factoriza y vencerás*. En estas tres palabras se guarda toda una filosofía de trabajo en investigación en teoría de números algebraicos.

2. Antecedentes en $\mathbb{Z}$

Usualmente se define un número primo p en $\mathbb{Z}$ como aquel entero $\neq 0, \pm 1$ con la propiedad: si $p = ab$, entonces $a = \pm 1$. Acto seguido, se justifica fácilmente por medio de inducción (por ejemplo), que cualquier entero $\neq\ 0, \pm 1$ admite al menos un divisor primo. Para justificar la unicidad en la factorización se utiliza el siguiente resultado:

Lema 2.1. *Si p es un número primo y $p \mid ab$, entonces $p \mid a$ o $p \mid b$.*

En realidad, la definición de número primo y el Lema 2.1 son equivalentes, al menos en $\mathbb{Z}$.

Teorema 2.2. *Sea $n \neq 0, \pm 1$ un entero con la siguiente propiedad: siempre que $n \mid ab$ implica $n \mid a$ o $n \mid b$. Entonces n es un número primo.*

La justificación no la podemos omitir: si $n = ab$ es una factorización de n, en particular $n \mid ab$. Por lo tanto $n \mid a$ o $n \mid b$. Si $n \mid a$ se tiene que $a = nt$, para algún $t \in \mathbb{N}$. Así que $n = ab = ntb$. De lo anterior se sigue que $b = 1$ y n es primo. Juntando el Lema 2.1 y el Teorema 2.2 tenemos la equivalencia.

Esta agradable coincidencia nos permite establecer las siguientes definiciónes, que por el momento significan lo mismo (en $\mathbb{Z}$).

Definición 2.3. *Sea p un entero $\neq 0, \pm 1$.*

1. *p es primo si $p \mid ab$, entonces $p \mid a$ o $p \mid b$.*
2. *p es irreducible si $p = ab$, entonces $p = a$ o $p = b$.*

Teorema 2.4. [Teorema Fundamental de la Aritmética.] *Cualquier $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ se puede escribir en forma única (salvo el orden de los factores)*

$$n = (-1)^{\lambda(n)} p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r},$$

donde $p_1, \ldots, p_r$ son números primos, $\lambda(n) = \pm 1$ según si $n > 0$ o $n < 0$ y $\lambda_i \in \mathbb{N}$.

Una consecuencia inmediata es que si $ab = c^n$ y $\text{mcd}(a, b) = 1$, entonces a y b también son potencias n-ésimas de ciertos enteros.

Si leemos con cuidado notaremos que en la definición de irreducible está implícita la presencia de ± 1, es decir, los únicos enteros que tienen inverso multiplicativo. En general, en cualquier anillo conmutativo no trivial A con 1 se tiene que el conjunto:

$$U(A) = \{a \in A : ax = 1 \text{ es soluble en } A\},$$

es un grupo abeliano, conocido como el *grupo de unidades* de A y en general no es fácil de calcularlo. Diremos que el anillo en cuestión es un *dominio de factorización única* (DFU) si es un dominio entero y si la factorización de cualquier elemento no cero y no unidad se puede escribir en forma única como producto de irreducibles o primos, salvo asociados. Es claro que en cualquier caso, $\pm 1 \in U(A)$. Veamos algunos ejemplos en donde es relativamente fácil encontrar $U(A)$.

1. $U(\mathbb{Z}) = \{1, -1\}$.
2. Si $\mathbb{Z}[2i] = \{a + 2bi : a, b \in \mathbb{Z}\}$, entonces $U(\mathbb{Z}[2i]) = \{1, -1\}$.
3. Si $\mathbb{Z}[\rho] = \left\{a + b\rho : a, b \in \mathbb{Z},\ \rho = \dfrac{-1 + i\sqrt{3}}{2}\right\}$, entonces $U(\mathbb{Z}[\rho]) = \{\pm 1, \pm\rho, \pm\rho^2\}$.

4. Si $\mathcal{O}_7 = \{a + b\sqrt{7} : a, b \in \mathbb{Z}\}$, entonces $U(\mathcal{O}_7) = \{\delta(8 + 3\sqrt{7})^n : n \in \mathbb{Z}, \delta = 1, -1\}$. El anillo $\mathcal{O}_7$ es un DFU pues es euclidiano.
5. Si K es un campo y $K[x]$ denota al anillo de polinomios con coeficientes en K, entonces $U(K[x]) = K \setminus \{0\}$.
6. Si $\mathbb{F}_{37}$ denota al campo finito con 37 elementos y $\mathbb{F}_{37}[x^3, x^5] = \{\sum a_{ij}x^{3i}x^{5j} : a_{ij} \in \mathbb{F}_{37}\}$, entonces $\mathbb{F}_{37}[x^3, x^5]$ es un subanillo de $\mathbb{F}_{37}[x]$ y $U(\mathbb{F}_{37}[x^3, x^5]) = \mathbb{F}_{37} \setminus \{0\}$. No es DFU pues por ejemplo $x^{15} = (x^3)^5 = (x^5)^3$ son dos factorizaciones *diferentes* de x^{15}.

En álgebra existen otros ejemplos importantes de anillos no conmutativos en donde es fácil identificar el grupo de unidades. Por ejemplo, el más importante de ellos es el anillo de matrices con entradas en un campo o un anillo. Concretamente, si K es un campo y $n \geq 2$, entonces:

$$U(M_{n\times n}(K)) = \{\text{matrices invertibles}\},$$

y claramente $U(M_{n\times n}(K))$ no es abeliano. En el caso particular de matrices de tamaño 3×3 el subgrupo de matrices ortogonales $O(3)$ y el subgrupo de $SO(3)$ de las matrices que además preservan orientación $SO(3)$, juegan un papel importante en otras disciplinas de la matemática.

Alteramos un poco la Definición 2.3 para destacar la importancia de conocer al grupo $U(A)$.

Definición 2.5. *Sea A un dominio entero con 1 y $U(A)$ el grupo de unidades de A. Sea $\pi \notin U(A), \pi \neq 0$.*

1. *π es primo si $\pi \mid ab$, entonces $\pi \mid a$ o $\pi \mid b$.*
2. *π es irreducible si $\pi = ab$, entonces $a \in U(A)$ o $b \in U(A)$.*

De la definición de irreducible tenemos que un elemento $\pi \notin U(A), \pi \neq 0$ es reducible si existen $a, b \in A$ tal que $\pi = ab$ y $a, b \notin U(A)$. También destacamos que si π es irreducible o primo y $u \in U(A)$, entonces $u\pi$ tiene la misma cualidad que π.

Lema 2.6. *Si π es primo, entonces π es irreducible.*

La justificación del lema anterior es prácticamente la misma que la del Teorema 2.2. Sabemos que en $\mathbb{Z}$ un elemento irreducible también es primo. Consideremos el anillo:

$$\mathbb{Z}[\sqrt{-19}] = \{a + b\sqrt{-19} : a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

En $\mathbb{Z}[\sqrt{-19}]$ tenemos toda la teoría de divisibilidad que conocemos en $\mathbb{Z}$ y sin embargo suceden cosas como las siguientes:

1. $U(\mathbb{Z}[\sqrt{-19}]) = \{1, -1\}$.
2. $35 = 5 \cdot 7 = (4 + \sqrt{-19})(4 - \sqrt{-19})$.
3. $5, 7, 4 + \sqrt{-19}$ y $4 - \sqrt{-19}$ son irreducibles y no primos en el anillo $\mathbb{Z}[\sqrt{-19}]$.
4. Cualesquiera dos números de $5, 7, 4 + \sqrt{-19}$ y $4 - \sqrt{-19}$ no son asociados.

La afirmación 2 es fácilmente verificable. Para las otras afirmaciones usaremos la función norma $\mathbf{N} : \mathbb{Z}[\sqrt{-19}] \longrightarrow \mathbb{N} \cup \{0\}$ definida como:

$$\mathbf{N}(a + b\sqrt{-19}) = a^2 + 19b^2.$$

Observamos que $(a + b\sqrt{-19})(a - b\sqrt{-19}) = a^2 + 19b^2$ y por lo tanto si $\alpha, \beta \in \mathbb{Z}[\sqrt{-19}]$ tenemos

$$\mathbf{N}(\alpha\beta) = \mathbf{N}(\alpha)\mathbf{N}(\beta).$$

Así, $\alpha \in U(\mathbb{Z}[\sqrt{-19}])$ si y sólo si $\mathbf{N}(\alpha) = 1$ y de esta afirmación se sigue inmediatamente 1 y 4. Ahora veremos que 5 es un elemento irreducible y no primo en el anillo $\mathbb{Z}[\sqrt{-19}]$. Supongamos que $5 = (a + b\sqrt{-19})(x + y\sqrt{-19})$. Entonces

$$\mathbf{N}(5) = 25 = (a^2 + 19b^2)(x^2 + 19y^2).$$

Así que:

$$a^2 + 19b^2 = x^2 + 19y^2 = 5$$

o

$$a^2 + 19b^2 = 1 \text{ y } x^2 + 19y^2 = 25.$$

En el primer caso $b = y = 0$ y $a^2 = x^2 = 5$ son ecuaciones no solubles en $\mathbb{Z}$. Así que $a^2 + 19b^2 = 1$ y $y^2 + 19y^2 = 25$. Por tanto $a + b\sqrt{-19} \in U(\mathbb{Z}[\sqrt{-19}])$ y 5 es irreducible. Ahora, si 5 fuera primo, entonces necesariamente

$$5 \mid 4 + \sqrt{-19} \quad \text{o} \quad 5 \mid 4 - \sqrt{-19}.$$

Si $5 \mid 4+\sqrt{-19}$, tenemos $4+\sqrt{-19} = 5(a+b\sqrt{-19})$ para algún $a + b\sqrt{-19} \in \mathbb{Z}[\sqrt{-19}]$. Igualando parte real y parte imaginaria $4 = 5a$ lo cual es imposible en $\mathbb{Z}$. Análogamente si $5 \mid 4 - \sqrt{-19}$. Por tanto 5 no es primo.

El anillo $\mathbb{Z}[\sqrt{-19}]$ está contenido en un anillo más grande en donde sí se cumple la propiedad de la factorización única. De hecho, $\mathbb{Z}[\sqrt{-19}]$ es un subgrupo máximo de índice 2 en el anillo $\mathcal{O}_{-19} = \{a + b\Big(\frac{-1 + \sqrt{-19}}{2}\Big) : a, b \in \mathbb{Z}\}$. Este fenómeno se debe a la aparición de nuevos *primos* en $\mathcal{O}_{-19}$ o dicho de otra manera, el anillo $\mathbb{Z}[\sqrt{-19}]$ no tiene suficientes elementos *primos*. Es destacable la importancia de la función norma. Aquí aparece un problema interesante: dado un dominio entero A que no es DFU, existe B DFU tal que $A \hookrightarrow B$. Parte de este problema corresponde a una rama avanzada de la Teoría de Números Algebraicos conocida como *Teoría de Campos de Clase*. Desafortunadamente no es posible dar una introducción en este trabajo pero invitamos al lector interesado para que consulte [11, páginas 146-147]. Por lo pronto, el lector puede empezar a sospechar que en la factorización única interviene fuertemente la coincidencia entre el concepto de elemento irreducible y elemento primo.

3. Anillos de interés en teoría de números algebraicos

En esta sección precisamos el estudio de la factorización única en algunos anillos de interés en la Teoría de Números. Si $\mathbb{F}$ es una extensión de grado 2 del campo de los números racionales $\mathbb{Q}$, entonces $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, donde $d \neq 0$ es un entero libre de cuadrados. Consideremos $M(\mathbb{Z}[x])$ el semigrupo formado por los polinomios mónicos con coeficientes enteros y $\mathbb{A} = \{\alpha \in \mathbb{C} : f(\alpha) = 0, \text{para algún } f(x) \in M(\mathbb{Z}[x])\}$ el anillo de enteros algebraicos. Definimos $\mathcal{O}_d = \mathbb{F} \cap \mathbb{A}$. Se sabe que si $d \equiv 2, 3 \pmod 4$, entonces

$$\mathcal{O}_d = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\},$$

y si $d \equiv 1 \pmod 4$, entonces

$$\mathcal{O}_d = \{a + b\Big(\frac{-1 + \sqrt{d}}{2}\Big) : a, b \in \mathbb{Z}\}.$$

El anillo $\mathcal{O}_d$ es conocido como el *anillo de enteros algebraicos* de $\mathbb{Q}(\sqrt{d})$. Debido a que el cociente $\mathcal{O}_d/I$ es finito, para cualquier ideal $I \neq 0$ de $\mathcal{O}_d$, se sigue que sólo existe un número finito de ideales de $\mathcal{O}_d$ que contienen a I. Por lo anterior, los anillos $\mathcal{O}_d$ son

noetherianos. Véase por ejemplo [5, página 189]. Notamos que en cualquier caso $\mathbb{Z} \subset \mathcal{O}_d$ y si $d = 1$, entonces $\mathcal{O}_1 = \mathbb{Z}$.

Por otro lado, $\mathbb{F}/\mathbb{Q}$ es una extensión de Galois con grupo de Galois $G = \{\mathrm{id}, \sigma\}$, donde $\sigma(\alpha) = \overline{\alpha}$ y $\overline{\alpha}$ es la conjugación racional:

$$\overline{a + b\sqrt{d}} = a - b\sqrt{d},$$

$$\overline{a + b\Big(\frac{-1+\sqrt{d}}{2}\Big)} = a + b\Big(\frac{-1-\sqrt{d}}{2}\Big).$$

La función $\mathbf{N} : \mathcal{O}_d \to \mathbb{Z}$ definida como $\mathbf{N}(\alpha) = \alpha\overline{\alpha}$ es lo que conocemos como *norma*. La propiedad más sobresaliente de la función norma y que se deduce fácilmente de la definición anterior es

$$\mathbf{N}(\alpha\beta) = \mathbf{N}(\alpha)\mathbf{N}(\beta),$$

en particular $\mathbf{N}(\pm 1) = 1$. Dependiendo del valor d, ésta toma la siguiente forma: Si $d \equiv 2, 3 \pmod 4$, entonces

$$\mathbf{N}(a + b\sqrt{d}) = a^2 - db^2,$$

y si $d \equiv 1 \pmod 4$, la norma toma la forma de una hipérbola. Concretamente:

$$\mathbf{N}\Big(a + b\Big(\frac{-1+\sqrt{d}}{2}\Big)\Big) = a^2 - ab + b^2\Big(\frac{1-d}{4}\Big).$$

Notamos que en cualquier caso $\mathbf{N}(\alpha) \in \mathbb{Z}$. En cualquier anillo $\mathcal{O}_d$ si $\mathbf{N}(\alpha) = p$, donde p es algún número primo, necesariamente α es un elemento irreducible. En efecto, pues si $\alpha = \beta\gamma$, entonces

$$\mathbf{N}(\alpha) = \mathbf{N}(\beta)\mathbf{N}(\gamma) = p,$$

y como ésta ya es una factorización en $\mathbb{Z}$, necesariamente $\mathbf{N}(\beta) = \pm 1$ o $\mathbf{N}(\gamma) = \pm 1$ y así β o γ es unidad. En esta dirección, si queremos encontrar irreducibles, podemos pensar en resolver la ecuación $\mathbf{N}(\alpha) = p$. Por ejemplo, en el anillo de enteros gaussianos $\mathcal{O}_{-1}$ los primos $p \in \mathbb{Z}$ de la forma $4n + 1$ se pueden escribir $p = a^2 + b^2$. Si aprovechamos la factorización en $\mathcal{O}_{-1}$:

$$p = a^2 + b^2 = (a + bi)(a - bi) = \mathbf{N}(a + bi),$$

tenemos que $a + bi$ es irreducible. De paso notamos que los primos en $\mathbb{Z}$ de la forma $4n + 1$ ya se pueden factorizar en $\mathcal{O}_{-1}$. Si identificamos $a^2 + b^2$ con la pareja (a, b), entonces las parejas (a, b) y (b, a) son *iguales*. Por otro lado, se sabe que existe una infinidad de primos racionales de la forma $4n + 1$, así que para cada primo de esta forma, la ecuación $\mathbf{N}(x + yi) = p$ tiene cuatro soluciones en los enteros x, y. Concretamente, las soluciones son las parejas:

$$(x, y),\ (-x, y),\ (x, -y),\ (-x, -y),$$

que esencialmente son las *mismas*, es decir, si (x, y) es solución y $u \in U(\mathcal{O}_{-1})$, entonces $u(x, y)$ también es solución. Lo anterior muestra parte de la importancia de conocer al grupo de unidades.

Teorema 3.1. *Si $d < 0$, entonces $U(\mathcal{O}_d)$ es un grupo finito descrito por:*

- $U(\mathcal{O}_{-1}) = \{\pm 1, \pm i\}$.
- $U(\mathcal{O}_{-3}) = \{\pm 1, \pm\rho, \pm(1 + \rho) : \rho^3 = 1,\ \rho \neq 1\}$.
- $U(\mathcal{O}_d) = \{\pm 1\}$ *si* $d = -2$ *o* $d < -3$.

El caso $d > 1$ y $d \equiv 2, 3 \pmod 4$ es más delicado, se tiene que resolver una ecuación de Pell $x^2 - dy^2 = \pm 1$. En general $x^2 - dy^2 = 1$ siempre tiene solución y $x^2 - dy^2 = -1$ depende de la paridad del período l de la representación en fracción continua de $\sqrt{d}$: si l es impar, $x^2 - dy^2 = -1$ es soluble y si l es par, entonces no existen unidades con norma -1. Se puede mostrar que existen $x, y > 0$ mínimos tal que cualquier solución positiva a, b satisface $a + b\sqrt{d} = (x + y\sqrt{d})^n$, para algún $n \in \mathbb{Z}$. La solución mínima positiva $x + y\sqrt{d}$ se conoce como *solución fundamental* o *unidad fundamental* en el caso $d \equiv 2, 3 \pmod 4$, y el conjunto de soluciones positivas $\{(x + y\sqrt{d})^n : n \in \mathbb{Z}\}$ es un grupo cíclico infinito cuyo generador es $x + y\sqrt{d}$. Una vez que conocemos la unidad fundamental, el grupo de unidades de $\mathcal{O}_d$ queda descrito como:

$$U(\mathcal{O}_d) = \{\delta(x + y\sqrt{d})^n : \delta = \pm 1,\ n \in \mathbb{Z}\}.$$

El caso $d \equiv 1 \pmod 4$ es similar, con una pequeña variante: la unidad fundamental de $\mathcal{O}_d$ se puede escribir como $\dfrac{a + b\sqrt{d}}{2}$ con $a \equiv b \pmod 2$. Esta se obtiene de resolver una ecuación parecida a la de Pell: $x^2 - dy^2 = 4$ con $x \equiv y \pmod 2$. Así por ejemplo, la unidad fundamental de $\mathcal{O}_{13}$ es $\dfrac{3 + \sqrt{13}}{2}$. Véase el libro [11, páginas 170-175].

No se conoce una descripción completa de $U(\mathcal{O}_d)$ para $d > 0$, tal como se da en el Teorema 3.1. Sin embargo, el famoso Teorema de la Unidades de Dirichlet nos describe la estructura aritmética de cualquier grupo de unidades en un anillo de enteros. En particular, para los campos cuadráticos reales tenemos:

Teorema 3.2. [Teorema de las Unidades de Dirichlet (caso cuadrático)] *Sea $d > 0$ y $\mathcal{O}_d$ el anillo de enteros de $\mathbb{Q}(\sqrt{d})$. Entonces existe $u \in U(\mathcal{O}_d)$ tal que cualquier $v \in U(\mathcal{O}_d)$ es de la forma $\pm u^n$, para algún $n \in \mathbb{Z}$.*

El elemento u del teorema anterior es precisamente la *unidad fundamental* y como mencionamos antes, el único camino *eficiente* para llegar a ella es por medio de las fracciones continuas. Así, en el ejemplo 4 de la sección 2 la unidad fundamental es $8 + 3\sqrt{7}$ y $\mathbf{N}(\delta(8 + 3\sqrt{7})^n) = 1$. La asignación $(\delta(8 + 3\sqrt{7})^n) \to (\delta, n)$ define un isomorfismo

$$\phi : U(\mathcal{O}_7) \to \{\pm 1\} \times \mathbb{Z}.$$

Para una demostración del Teorema de Dirichlet, en el caso cuadrático, el lector puede consultar la bella exposición en [5, páginas 191-192] y para una versión general, la cual no es fácil, invitamos a los interesados consultar [17, páginas 293-300].

Concentremos nuestra atención en el anillo cuadrático $\mathcal{O}_d$ con $d > 0$ y libre de cuadrados. En $\mathcal{O}_d$ existe una infinidad de elementos irreducibles, lo cual da la posibilidad de factorizar en irreducibles cualquier elemento $\neq 0$ y no unidad. El *discriminante* de $\mathbb{Q}(\sqrt{d})$ lo definimos como $\delta = 4d$ si $d \equiv 2, 3 \pmod 4$ o $\delta = d$ si $d \equiv 1 \pmod 4$. Cualquiera que sea el caso, cualquier ideal $0 \neq I \subset \mathcal{O}_d$ se puede escribir de manera única en alguna de las siguientes formas:

$$I = \mathcal{P}, \mathcal{P}^2, \mathcal{P}_1\mathcal{P}_2,$$

donde $\mathcal{P}, \mathcal{P}_1, \mathcal{P}_2$ son ideales primos en $\mathcal{O}_d$. En particular, si p es un primo impar, $p \nmid \delta$ y el símbolo de Legendre $\left(\dfrac{d}{p}\right) = -1$, entonces el ideal principal $p\mathcal{O}_d$ tiene la factorización $p\mathcal{O}_d = \mathcal{P}$ ([5] Proposition 13.1.3), mostrando con esto que el ideal primo $\mathcal{P}$ es principal.

Teorema 3.3. *En un dominio entero con 1, los ideales principales primos son generados por elementos primos y los ideales principales máximos son generados por elementos irreducibles.*

Demostración: Sea $\mathcal{P}$ un ideal primo principal. Si $\mathcal{P} =< \pi >$ y $\pi \mid ab$, entonces $ab \in \mathcal{P}$ y por lo tanto $a \in \mathcal{P}$ o $b \in \mathcal{P}$. Así que

$a = \pi q$ o $b = \pi t$. Esto significa que $\pi \mid a$ ó $\pi \mid b$. Por lo tanto π es primo. La segunda afirmación es un ejercicio fácil para el lector.

Notamos que la primera afirmación del Teorema 3.3 es válida si sólo pedimos que el anillo sea conmutativo con 1, así, los ideales primos principales en $\mathcal{O}_d$ están generados por elementos primos y por tanto, por elementos irreducibles. Usando la Ley de Reciprocidad Cuadrática es fácil deducir que existe una infinidad de primos impares p tal que $p \nmid \delta$ y $\left(\frac{d}{p}\right) = -1$. Así tenemos:

Teorema 3.4. [Teorema de Euclides para $\mathcal{O}_d$] *Existe una infinidad de irreducibles en el anillo $\mathcal{O}_d$.*

Si $d > 0$ y libre de cuadrados, entonces cada irreducible π en $\mathcal{O}_d$ tiene una infinidad de asociados: $\pi U(\mathcal{O}_d)$. Ahora que ya sabemos que existen suficientes irreducibles en $\mathcal{O}_d$, vamos a darles el uso adecuado.

Teorema 3.5. *Cualquier elemento $a \in \mathcal{O}_d \setminus \{0\}$ que no es unidad admite al menos un divisor irreducible.*

Demostración: Si a es irreducible no hay nada que mostrar pues $a \mid a$. Así que podemos suponer que $a = t_1 t_2$, con $t_1, t_2 \notin U(\mathcal{O}_d)$. Así tenemos la contención propia de ideales

$$\langle a \rangle \subset \langle t_1 \rangle.$$

Si t_1 o t_2 es irreducible, terminamos. Si t_1 y t_2 son reducibles, entonces $t_1 = t_{11}t_{12}$, $t_2 = t_{21}t_{22}$ y por tanto $a = t_{11}t_{12}t_{21}t_{22}$. Si algún t_{ij} es irreducible terminamos. De otra forma tenemos la cadena de ideales

$$\langle a \rangle \subset \langle t_1 \rangle \subset \langle t_{11} \rangle.$$

Si el proceso continua, estamos generando una cadena ascendente de ideales que en algún momento debe detenerse por ser $\mathcal{O}_d$ noetheriano:

$$\langle a \rangle \subset \langle t_1 \rangle \subset \langle t_{11} \rangle \subset \cdots \subset \langle t \rangle \subset \mathcal{O}_d,$$

y t necesariamente es irreducible.

El lector puede reconocer en el argumento de la prueba anterior, las mismas ideas cuando se intenta demostrar que cualquier entero $\neq 0, \pm 1$ admite al menos un divisor primo.

Corolario 3.6. *Cualquier elemento $a \in \mathcal{O}_d \setminus \{0\}$ es una unidad o se puede escribir como producto finito de irreducibles y unidades.*

Demostración: Si a no es unidad y reducible, entonces $a = \pi_1 b$, para algún $b \in \mathcal{O}_d$. Se repite el argumento con b y al final se llega a que $a = \pi_1 \pi_2 \cdots \pi_r u$, donde u es alguna unidad.

Es una ventaja saber que se puede factorizar y en cualquier caso es suficiente factorizar cualquier primo racional que aparece en la factorización de la norma de un entero algebraico. Veamos un algoritmo en el anillo de los enteros gaussianos $\mathcal{O}_{-1} = \mathbb{Z}[i]$. Las siguientes afirmaciones son conocidas en $\mathbb{Z}[i]$ ([9, páginas 81-82]):

1. $\mathbb{Z}[i]$ es un anillo euclidiano y por tanto es un DFU.
2. Los primos racionales de la forma $4n + 1$ se pueden escribir como $p = a^2 + b^2$.
3. Los primos en $\mathbb{Z}[i]$ son:
   i) $1 + i$ y $i - 1$.
   ii) Los primos racionales de la forma $4n + 3$.
   iii) Los factores $a+bi$ de primos racionales de la forma $4n+1$.

Claramente si $u \in U(\mathbb{Z}[i])$ y π es alguno de los primos mencionados en la lista anterior, entonces $u\pi$ también es primo. Sea $z \in \mathbb{Z}[i]$ y $\mathbf{N}(z) = n$. Cualquier factor primo del número z es un factor primo de su norma $n = z\bar{z}$. Los factores primos gaussianos del entero n pueden encontrarse fácilmente obteniendo sus factores primos racionales.

Consideremos la siguiente factorización en $\mathbb{Z}$:

$$n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s} \tag{1}$$

donde los p_i y q_j son primos racionales de la forma $4n+1$ y $4n+3$ respectivamente. Si $p_i = \pi_i \bar{\pi}_i$ con $i = 1, ..., r$, entonces la factorización de n en $\mathbb{Z}[i]$ es:

$$n = i^{\alpha}(1-i)^{2\alpha} \prod_{i=1}^{r} \pi_i^{\alpha_i} \bar{\pi}_i^{\alpha_i} \prod_{i=1}^{s} q_i^{\beta_i} \tag{2}$$

Puesto que $z \mid n$, necesariamente

$$z = i^{\delta}(1+i)^{\lambda} \prod_{i=1}^{r} \pi_i^{a_i} \bar{\pi}_i^{a_i'} \prod_{i=1}^{s} q_i^{\mu_i} \tag{3}$$

donde $\delta \in \{1, 2, 3, 4\}$ y $\lambda, a_i, a_i', \mu_i \geq 0$.

Por otro lado $\mathbf{N}(\pi_j) = p_j$ y $\mathbf{N}(q_i) = q_i^2$, así que tomando normas en (3) obtenemos

$$\mathbf{N}(z) = 2^{\lambda} p_1^{a_1 + a_1'} p_2^{a_2 + a_2'} \cdots p_r^{a_r + a_r'} q_1^{2\mu_1} q_2^{2\mu_2} \cdots q_s^{2\mu_s}.$$

Comparando los exponentes de esta última expresión con (1)

$$\lambda = \alpha, \quad a_i + a_i' = \alpha_i, \quad 2\mu_i = \beta_i.$$

De lo anterior tenemos que: Si un entero positivo n es norma de algún gaussiano, entonces en la factorización de n en primos racionales, los primos de la forma $4n + 3$ aparecen con exponente par.

Nuestro trabajo aún está incompleto pues sólo hemos encontrado los exponentes de los primos racionales de la forma $4n + 3$. Para obtener la factorización completa de z debemos determinar los números a_j, a_j'.

Sea k_j el mayor entero no negativo para el cual $p_j^{k_j} \mid z$. Afirmamos que:

$$\text{si} \quad p_j^{k_j} \pi_j \mid z, \quad \text{entonces} \quad \begin{cases} a_j &= \alpha_j - k_j \\ a_j' &= k_j, \end{cases}$$

$$\text{si} \quad p_j^{k_j} \pi_j \nmid z, \quad \text{entonces} \quad \begin{cases} a_j &= k_j \\ a_j' &= \alpha_j - k_j. \end{cases}$$

Según nuestra definición de k_j, tenemos que $\frac{z}{p_j^{k_j}}$ no puede ser dividido simultáneamente por π_j y $\bar{\pi}_j$ porque si esto sucediera entonces $\pi_j \bar{\pi}_j$ debe dividir a $\frac{z}{p_j^{k_j}}$ pues $\text{mcd}(\pi_j, \bar{\pi}_j) = 1$ y así $p_j^{k_j+1} \mid z$, lo cual no es posible por la elección de k_j. Resumiendo, si π_j es divisor de $\frac{z}{p_j^{k_j}}$, entonces $\bar{\pi}_j$ no es divisor de $\frac{z}{p_j^{k_j}}$. Por otro lado, $p_j^{k_j} = \pi_j^{k_j} \bar{\pi}_j^{k_j}$. Haciendo uso de la expresión

$$z = i^{\delta}(1+i)^{\lambda} \pi_1^{a_1} \bar{\pi}_1^{a_1'} \pi_2^{a_2} \bar{\pi}_2^{a_2'} \cdots \pi_r^{a_r} \bar{\pi}_r^{a_r'} q_1^{\mu_1} \cdots q_s^{\mu_s},$$

concluimos que $a_j' = k_j$ y $a_j = \alpha_j - k_j$.

Un razonamiento similar muestra que si π_j no divide a $\dfrac{z}{p_j^{k_j}}$, entonces $a_j = k_j$ y $a_j' = \alpha_j - k_j$.

Por último, el exponente δ puede ser calculado haciendo una simple división de z y el producto de los factores primos para los cuales sus exponentes ya han sido encontrados. Antes de aplicar lo anterior en un ejemplo específico debemos notar que no todo es tan fácil: la factorización de n en (1) puede resultar bastante complicada pues no hay métodos eficientes para factorizar en $\mathbb{Z}$.

Ejemplo 3.7. *Sea $z = 22 + 7i$. Entonces $\mathbf{N}(z) = 484 + 49 = 13 \cdot 41$. Escribimos $p_1 = 13 = 2^2 + 3^2$ y $p_2 = 41 = 4^2 + 5^2$. Por lo tanto $\alpha_1 = 1$, $\alpha_2 = 1$ y*

$$z = i^{\delta}\pi_1^{a_1}\bar{\pi}_1^{a_1'}\pi_2^{a_2}\bar{\pi}_2^{a_2'},$$

donde $\pi_1 = 2 + 3i$, $\bar{\pi}_1 = 2 - 3i$, $\pi_2 = 4 + 5i$, $\bar{\pi}_2 = 4 - 5i$.

Sólo nos falta encontrar los exponentes a_1, a_1', a_2, a_2'. Como $p_1 \nmid z$ y $p_2 \nmid z$, entonces $k_1 = k_2 = 0$. Ahora veamos si $\pi_1 \mid z$ o $\bar{\pi}_1 \mid z$:

$$\frac{z}{\pi_1} = \frac{22 + 7i}{2 + 3i} = 5 - 4i,$$

así que $\bar{\pi}_1 \nmid z$ y por lo tanto $a_1 = 1$ y $a_1' = 0$. Análogamente, de la igualdad

$$\frac{z}{\pi_2} = \frac{22 + 7i}{4 + 5i} = 3 - 2i,$$

se obtiene $\bar{\pi}_2 \nmid z$ y por lo tanto $a_2 = 1 - 0$ y $a_2' = 0$.

Hasta ahora hemos obtenido que $z = i^{\delta}(2 + 3i)(4 + 5i)$. Con una simple división vemos que $\delta = 3$ y así $z = i^3(2 + 3i)(4 + 5i)$.

Como puede notar el lector, factorizar en los anillos $\mathcal{O}_d$ resulta bastante complicado. En nuestro ejemplo el anillo es DFU y esto es una ayuda definitiva. El método descrito funciona si la norma del gaussiano no es muy grande, digamos que se pueda factorizar con alguno de los métodos modernos de factorización de enteros.

Finalizamos la sección con el objetivo principal de este trabajo:

Teorema 3.8. *El anillo $\mathcal{O}_d$ es DFU si y sólo si primo e irreducible coinciden.*

Demostración: Véase [17, páginas 87-88].

No es común utilizar el Teorema 3.8 para identificar que cierto dominio entero es DFU; se tienen otras alternativas. Por ejemplo se puede intentar mostrar que es euclidiano, que es de ideales principales y en el caso de anillos de enteros se puede intentar mostrar que el *número de clase* es 1. Para una definición del número de clase de un anillo de enteros véase [5, Capítulo 12]. El problema de determinar todos los anillos cuadráticos que son DFU es un problema abierto.

4. Factorizaciones raras

1. En el anillo $\mathbb{Z}_6[x]$ tenemos la factorización $x = (3x+4)(4x+3)$ y por tanto el polinomio x no es irreducible $\mathbb{Z}_6[x]$ como sucede en $K[x]$ donde K es cualquier campo.
2. Consideremos el semigrupo $S = \{x \in \mathbb{N} : x \equiv 1 \pmod 7\}$. Diremos que un elemento $x \in S$ es *primo* si $x = ab$ con $a, b \in S$, entonces $a = x$ ó $b = x$. Por ejemplo $22, 8$ y 1331 son primos en S y

   $$10648 = 22 \cdot 22 \cdot 22 = 8 \cdot 1331$$

   son dos factorizaciones con un número diferente de *primos*.
3. Si K es un campo y $\text{mcd}(n, m) = 1$, entonces en el anillo $K[x^n, x^m] = \{\sum a_{ij}x^{ni}x^{mj} : a_{ij} \in K\} \subset K[x]$ se tiene que x^n y x^m son irreducibles y

   $$x^{mn} = x^n \cdot x^n \cdots x^n = x^m \cdot x^m \cdots x^m$$

4. Sea $A = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{Z} \right\}$. Entonces A es un semigrupo con el producto usual de matrices. Denotamos por (a) a cualquier elemento típico de A. Diremos que (a) es compuesto si $(a) = (y)(z)$ y $(y), (z) \in A$. En caso contrario diremos que (a) es "primo". Un simple cálculo muestra que $(y)(z) = (2yz)$. Se puede observar que las matrices

   $$\begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} -11 & -11 \\ -11 & -11 \end{pmatrix}, \begin{pmatrix} 7 & 7 \\ 7 & 7 \end{pmatrix}$$

   son "primos.[en] A. Si $a = 2t$, entonces $(a) = (2t) = (1)(t)$ y (a) es compuesto. Inversamente si $(a) = (y)(z) = (2yz)$, entonces a es par. Por tanto (a) es "primo.[en] A si y sólo si a es impar. En general, si $x = 2^n q$ con q impar, se tiene:

   i) $a = 2q$, entonces $(a) = (1)(q) = (-1)(-q)$ y por tanto (a) tienen dos factorizaciones.

   ii) $a = 2^n q$ y $n > 1$, entonces $(a) = (1)^n(q) = (1)^{n-1}(-1)(-q)$ y (a) tiene dos factorizaciones.

   La única matriz que se puede factorizar en forma única es $(-2) = (-1)(1)$. Véase [4].
5. En el enunciado del Teorema 3.8 se puede reemplazar la frase ".[El] anillo $\mathcal{O}_d$"por "dominio entero con factorización". Veamos el siguiente ejemplo: Sea $\mathbb{Q}^{(2)} = \{\frac{a}{b} \in \mathbb{Q} : 2 \nmid b\}$. Entonces $\mathbb{Q}^{(2)}$ es un dominio entero contenido en $\mathbb{Q}$. Primero notemos que $\dfrac{a}{b} \in \mathbb{Q}^{(2)}$ es unidad si y sólo si $2 \nmid a$. Así, $\mathbb{Q}^{(2)}$ tiene una infinidad de unidades y 2 es irreducible. Por otro lado, si $\dfrac{a}{b} \neq 2$ es otro irreducible, entonces $a = 2t$ y $\dfrac{a}{b} = \dfrac{2}{1}\dfrac{t}{b}$. Puesto que $\dfrac{a}{b}$ es irreducible, necesariamente $\dfrac{t}{b}$ es unidad y así $\dfrac{a}{b}$ es asociado de 2. Por tanto, los únicos irreducibles son 2 y sus asociados. Se puede verificar fácilmente que si $\dfrac{2t}{b}$ es irreducible, entonces $\dfrac{2t}{b}$ es primo y así, la factorización es única en $\mathbb{Q}^{(2)}$.

Referencias

1. Adams W. W., and Goldstein L. J., *Introduction to Number Theory*. Prentice-Hall 1976.
2. Edwards H.M., *Fermat's Last Theorem*, Springer Verlag GTM 50, 2000.
3. Hardy G.H., Wright E.M. *An introduction to the theory of numbers*. Oxford University Press, Oxford 1979.
4. Jacobson B., Matrix Number Theory: An example of nonunique factorization. American Mathematical Monthly, **72**, No. 4 (1965), 399-402.
5. Ireland K., Rosen M., *A classical introduction to modern number theory*. GTM **84** Springer Verlag 1982.
6. Lemmermeyer F., The Euclidean algorithm in algebraic number fields. Expositiones Mathematicae, **13** (1995), 385-416.
7. Nagell T., *Number theory*. AMS Chelsea 2001.
8. Niven I., Zuckerman S., Montgomery H.L., *An Introduction to the Theory of Numbers*. 5th ed., John Wiley, New York, 1991.
9. Pineda-Ruelas M., *Aritmética y Teoría de Números*. Universidad Autónoma Metropolitana, 1995.
10. Ribenboim P., *Números primos: mistérios e recordes*. Coleção Matemática Universitaria, Rio de Janeiro: IMPA 2001.
11. Ribenboim P., *Classical Theory of Algebraic Numbers*. Universitext, Springer, New York (2001).
12. Shanks D., *Solved and Unsolved Problems in Number Theory*. Chelsea, New York, 2002.
13. Sierpinski W., *Elementary theory of numbers*, Państowe Wydawnictwo Naukowe 1964.
14. Silverman J. H., *A friendly Introduction to number theory*. Prentice-Hall, 3 edition, New Jersey 2005.
15. Silvester J.R., *A Matrix Method for Solving Linear Congruences*. Mathematics Magazine, **53**, No. 2, 90-92 (1980).
16. Stark M.H., *An introduction to number theory*. MIT Press (1978).
17. Stewart I., Tall D., *Algebraic Number Theory and Fermat Last Theorem*. A K Peters, third edition, 2002.
18. Weil A., *Number theory: An approach through history from Hummurapi to Legendre*, Birkhäuser, Boston, 1984.

Agradezco al árbitro anónimo sus sugerencias porque mejoraron sustancialmente la presentación de este trabajo.

Euler y la Conjetura de Catalan

Arturo Cueto Hernández
arch@correo.azc.uam.mx
UAM-Azcapotzalco

1. Introducción

En 2002 el matemático rumano Preda Mihăilescu anunció una demostración completa de la Conjetura de Catalan. Sorprendentemente, su demostración tiene muy poco de cálculo computacional; en su lugar utiliza resultados teóricos profundos, principalmente de la teoría de campos ciclotómicos.

En este trabajo se presenta la parte histórica de la Conjetura de Catalan. En particular, daremos tres demostraciones de un teorema que responde parcialmente a la conjetura mencionada. Este teorema fue establecido por Euler en 1738 e indica que $x = 3$ y $y = 2$ son los únicos racionales positivos tales que $x^2 = y^3 + 1$.

2. Historia

La Conjetura de Catalan, hoy en día un teorema, fue uno de esos problemas en teoría de números que son fáciles de formular pero extremadamente difícil de resolver. La conjetura afirma que 8 y 9 son las únicas potencias exactas consecutivas. **Conjetura.** (E. Catalan, 1844)*Los únicos dos números consecutivos en la sucesión de potencias exactas de números naturales*

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, \\ 100, 121, 125, 128, 144, 169, 196, \ldots$$

son 8 *y* 9. En otras palabras, no existe otra solución de la ecuación diofántica

$$x^m - y^n = 1 \tag{1}$$

con $x > 1$, $y > 1$, $m > 1$ y $n > 1$ que la dada por $x^m = 3^2$, $y^n = 2^3$.

La historia de la Conjetura de Catalan comienza en el año de 1844, cuando el editor del *Journal für die Reine und Angewandte Mathematik (Crelle's Journal)* recibió una carta del matemático belga Eugène Charles Catalan (1814–1894). La revista publicó un extracto de ésta en 1844. El extracto fue el siguiente:

Note

extraite dúne lettre adressée à l'éditeur par Mr. E. Catalan, Répétiteur à l'école polytechnique de Paris.

> Je vous prie, Monsieur, de vouloir bien énoncer, dans votre recueil, le théorème suivant, que je crois vrai, bien que je náie pas encore réussi à le démontrer complètement: dáutres seront peut-être plus heureux:
>
> Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être des puissances exactes; autrement dit: l'équation $x^m - y^n = 1$, dans laquelle les inconnues sont entières et positives, nádmèt quúne seule solution.

Catalan fue profesor en La Escuela Politécnica de París, y obtuvo reputación por la solución de un problema de combinatoria. El término "número de Catalan", todavía en uso, se refiere a este problema combinatorio.

De acuerdo con Dickson [7], Catalan no fue el primero que consideró este problema diofántico, pero sí fue el primero en conjeturarlo en su forma general. Philippe de Vitry (1291–1361), quien fuera mejor conocido como compositor y músico teórico que como matemático, planteó el problema de la siguiente manera: todas las potencias de 2 y 3 difieren por más de una unidad, excepto para los pares 1 y 2, 2 y 3, 3 y 4, 8 y 9. Levi ben Gerson (1288–1344), quien fue también conocido como Gersonides, resuelve el problema demostrando que $3^m \pm 1$ siempre tiene un factor primo impar si $m > 2$; así, $3^m \pm 1$ no puede ser una potencia de 2. Euler resuelve la ecuación $x^2 - y^3 = 1$ en 1738 y demuestra que la única solución positiva es $x = 3$, $y = 2$.

El primer resultado acerca del problema fue publicado seis años después de la publicación de Catalan. El matemático francés Victor Amédée Lebesgue (1791–1875) [10] demostró que la ecuación $x^p - y^2 = 1$, donde p es un número primo, no tiene soluciones en enteros positivos x y y; Lebesgue usó enteros gaussianos para demostrarlo y al final de su artículo dice que otros casos de la ecuación $x^m = y^n + 1$ parecen presentar más dificultades y que desconoce si Catalan ha hallado algo al respecto. Pero Catalan no halló mucho, los únicos resultados que obtuvo fueron publicados en 1885. Catalan sólo hace algunas observaciones empíricas, las cuales establece sin demostración, esperando que otras personas pudieran hallarlas útiles. Las observaciones que menciona son casos especiales de la conjetura general, por ejemplo las ecuaciones $(x+1)^x - x^x = 1$, $x^y - y^x = 1$ y $x^p - q^y = 1$, donde p y q son primos.

Después del resultado de Lebesgue, todos los progresos consistieron en trabajos con exponentes pequeños. Nagell demostró

en 1921 que la diferencia entre una potencia cúbica y otra potencia exacta nunca es igual a 1. En 1932, Selberg demostró que $x^4 - y^n = 1$ no tiene solución en enteros positivos cuando $n > 1$. En 1965 Ko Chao [9] demostró que la ecuación $x^2 - y^q = 1$ no tiene solución en enteros positivos cuando $q \geq 5$, el cual es un resultado más fuerte que el de Selberg. En 1976 Chein [6] da una demostración más simple del Teorema de Chao, usando el hecho de que si $x^2 - y^q = 1$ con q primo y $x \geq 1$, $y \geq 1$, entonces 2 divide a y y q divide a x. Este último también es un resultado de Nagell.

El siguiente resultado que no trata con exponentes pequeños fue demostrado por LeVeque en 1952 [11]. Él estudió el número de soluciones de la ecuación de Catalan y demostró que la ecuación $x^a - y^b = 1$ tiene a lo más una para enteros dados a y b, a menos que $a = 2$, $b = 3$, en cuyo caso existen exactamente dos, a saber, $(3, 2)$ y $(-3, 2)$.

En 1953 y 1960 Cassels [2], [3] publicó algunos resultados acerca de la ecuación $x^p - y^q = 1$, donde p y q son primos impares. Él demostró que si esta igualdad se tiene para enteros positivos x y y, entonces p divide a y y q divide a x. El caso $p = 2$ ya había sido demostrado por Nagell. De los resultados de Cassels se sigue que tres enteros consecutivos no pueden ser potencias exactas, como A. Mąkowski [12] demostró en 1962.

Hyyrő también trabajó en la Conjetura de Catalan. Él refinó los resultados de Cassels en 1964, cuando da varias congruencias que se tienen para enteros x y y mayores que 1 y primos p y q tales que $x^p - y^q = 1$. Él obtiene una cota inferior del valor absoluto de x.

La teoría de Baker acerca de cotas efectivas para soluciones de ciertos tipos de ecuaciones diofánticas es aplicada a la ecuación de Catalan. En 1976, Tijdeman [18] usó la teoría de Baker y demostró que existe una cota superior calculable de los tamaños de p, q, x y y, donde p y q son primos y x y y son enteros tales que $x^p - y^q = 1$. Esto implica que la ecuación de Catalan tiene un número finito de soluciones.

Inkeri definió el concepto de un par Wieferich en el contexto de la ecuación de Catalan como sigue: un par Wieferich es un par (p, q) de primos tales que $p^{q-1} \equiv 1 \pmod{q^2}$ y $q^{p-1} \equiv 1 \pmod{p^2}$. En 1990, demostró que si la ecuación de Catalan $x^p - y^q = 1$ se cumple, entonces (p, q) es un par Wieferich, o q divide a h_p, el número de clase del campo ciclotómico $\mathbb{Q}(\zeta_p)$, o p divide a h_q, el número de clase de $\mathbb{Q}(\zeta_q)$. Bugeaud y Hanrot [1] dan un criterio acerca de la ecuación de Catalan usando el número de clase, el cual implica que la ecuación de Catalan $x^p - y^q = 1$ no tiene solución en enteros no cero x y y si p y q son primos tales que uno de ellos es menor que 43. Finalmente, Mihăilescu tuvo éxito en eliminar el criterio del número de clase demostrando que si la ecuación de Catalan se tiene, entonces (p, q) es un par Wieferich. Mihăilescu demostró que la ecuación de Catalan no tiene soluciones si p y q son impares y q no divide a $p-1$. También tuvo éxito en demostrar la Conjetura de Catalan en el caso cuando q divide a $p - 1$. Por lo anterior la Conjetura de Catalan es ahora un Teorema.

3. El Trabajo de Euler

En esta sección se estudiará el trabajo de Euler en relación a la Conjetura de Catalan. Primero daremos una demostración usando la teoría de curvas elípticas. Luego se presentará la demostración de Euler dada hace 269 años y se observará que esencialmente es la misma que la demostración basada en curvas elípticas. Por último, se dará una tercera demostración basada en teoría de anillos.

El trabajo de Euler en relación a la Conjetura de Catalan, es el siguiente teorema:

Teorema 3.1. (Euler 1738)
Si x y y son racionales positivos tales que $x^2 = y^3 + 1$, entonces $x = 3$ y $y = 2$.

En términos de la teoría de curvas elípticas, Euler halló los puntos con coordenadas racionales positivas en la curva elíptica $E : y^2 = x^3 + 1$. Viendo estos puntos como puntos afines de la curva proyectiva $y^2z = x^3 + z^3$. Junto con el punto $\mathcal{O} = (0, 1, 0)$ al infinito, los puntos afines forman un grupo aditivo con elemento identidad $\mathcal{O}$. Cabe mencionar que es un problema abierto exhibir un algoritmo para hallar los generadores del grupo de puntos racionales de una curva elíptica, aunque se puede hacer en instancias especiales. En este caso, el Teorema de Euler es implicado por el siguiente resultado:

Teorema 3.2.
El grupo de puntos racionales de la curva elíptica $y^2 = x^3 + 1$ es un grupo cíclico de orden 6 con elementos

$$\{(-1, 0), (0, 1), (0, -1), (2, 3), (2, -3), \mathcal{O}\}$$

donde $\mathcal{O}$ denota el punto al infinito.

3.1. Teoría de Curvas Elípticas

Se presenta a continuación la teoría de curvas elípticas que se usará para demostrar el Teorema 3.2, la demostración de estos resultados se puede consultar en el libro de Silverman–Tate [16].

Teorema 3.3. (Mordell–Weil)
El grupo de puntos racionales de una curva elíptica E es un grupo abeliano finitamente generado.

Es decir, este grupo es de la forma

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

donde $T = E(\mathbb{Q})_{tors}$, el subgrupo de torsión de $E(\mathbb{Q})$, es un grupo abeliano finito. El número r es el rango de la curva elíptica. Una de las partes más importantes en la demostración del Teorema de Mordell–Weil es que el índice $[E(\mathbb{Q}) : mE(\mathbb{Q})]$ es finito, para $m \in \mathbb{Z}$. Existe una noción del tamaño de un punto en el caso de las curvas elípticas, a saber: la altura del punto.

Definición 3.1.
Sea $x = \frac{v}{w}$ un número racional escrito en su forma reducida. Entonces la altura $H(x)$ de x se define como:

$$H(x) = H\left(\frac{v}{w}\right) = \text{máx}\{|v|, |w|\}.$$

Definición 3.2.
Se define la altura de un punto como la altura de la coordenada x del punto.

A continuación describimos los pasos generales que usaremos en la demostración del Teorema 3.2. El m que usaremos será 2. Sean $m = 2$ y $Q_1, Q_2, \ldots, Q_n$ representantes de las clases de $2E(\mathbb{Q})$. Así, para cualquier P en $E(\mathbb{Q})$, podemos escribir

$$P - Q_i = 2P',$$

para algún $i = 1 \ldots, n$ y para un punto $P' \in E(\mathbb{Q})$. Podemos hacer lo mismo con P', y así sucesivamente. La idea básica es que el "tamaño" de los puntos $P, P', P'', \ldots$ que obtenemos en esta forma sera más pequeño en cada paso.

Continuando el proceso indicado arriba, siempre llegamos a un punto $P^{(j)}$, para algún entero j, tal que la altura de $P^{(j)}$ es menor que un cierto entero dado κ. Como sólo existe un número finito de puntos con altura menor que un entero dado, se sigue que todos los puntos en $E(\mathbb{Q})$ son generados por el conjunto finito

$$\{Q_1, \ldots, Q_n\} \cup \{R \in E(\mathbb{Q}) \,:\, H(R) \leq \kappa\}$$

para algún entero κ.

El algoritmo que usaremos para la demostración usa más detalles de la demostración del Teorema de Mordell–Weil, [16]. Por ejemplo, el homomorfismo α que usaremos juega un papel importante en la demostración de la finitud del índice $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$.

Calcular $E(\mathbb{Q})/2E(\mathbb{Q})$ es relativamente fácil si $E(\mathbb{Q})$ tiene un punto racional de 2–torsión. Supongamos, después de un cambio de coordenadas $(x, y) \mapsto (x + e, y)$, que E es una curva elíptica dada por la ecuación

$$E \,:\, y^2 = x^3 + ax^2 + bx$$

y construyamos la curva E' dada por la ecuación:

$$E' \,:\, y^2 = x^3 + \overline{a}x^2 + \overline{b}x,$$

donde $\overline{a} = -2a$ y $\overline{b} = a^2 - 4b$.

Entonces existe una isógena $\varphi : E \to E'$ definida por

$$\varphi(P) = \begin{cases} \left(\dfrac{y^2}{x^2}, \dfrac{y(x^2-b)}{x^2}\right) & \text{si } P = (x, y) \neq \mathcal{O}, (0, 0) \\ \\ \overline{\mathcal{O}} & \text{si } P = \mathcal{O} \text{ o } P = (0, 0) \end{cases}$$

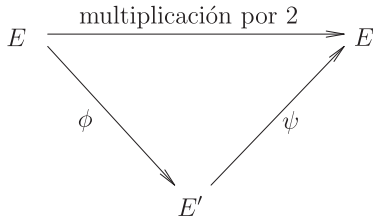
El kernel de φ es $\{\mathcal{O}, (0, 0)\}$.

Similarmente, construimos la curva E'' de E' y definimos el mapeo $\overline{\varphi} : E' \to E''$ similar a φ. La curva E'' es isomorfa a E vía el mapeo $(x, y) \to \left(\dfrac{x}{4}, \dfrac{y}{8}\right)$. Existe así una isógena dual $\psi : E' \to E$ definida por

$$\psi(\overline{P}) = \begin{cases} \left(\dfrac{\overline{y}^2}{4\overline{x}^2}, \dfrac{\overline{y}(\overline{x}^2 - \overline{b})}{8\overline{x}^2}\right) & \text{si } \overline{P} = (\overline{x}, \overline{y}) \neq \overline{\mathcal{O}}, (\overline{0}, \overline{0}) \\ \\ \mathcal{O} & \text{si } \overline{P} = \overline{\mathcal{O}} \text{ o } \overline{P} = (\overline{0}, \overline{0}) \end{cases}$$

La composición $\psi \circ \varphi : E \to E$ es multiplicación por 2: $\psi \circ \varphi(P) = 2P$ para todos los puntos P en $E(\mathbb{Q})$.

El siguiente diagrama muestra la situación:



Teorema 3.4. (Nagell–Lutz)
Si $P = (x, y)$ es un punto racional de orden finito en una curva elíptica E, y Δ es el discriminante del polinomio cúbico que define a E, entonces x y y son enteros, y $y = 0$ ó y^2 divide a Δ.

3.2. Demostración con Curvas Elípticas

El objetivo de la demostración es probar que el rango de la curva elíptica $y^2 = x^3 + 1$ es 0. Para establecer esto usaremos un método 2–descendente. La parte correspondiente a T es relativamente fácil.

Demostración Teorema 3.2:
Consideremos la curva elíptica D dada por la ecuación de Weierstrass

$$y^2 = x^3 + 1.$$

Primero, cambiemos las coordenadas de tal forma que el punto racional de 2–torsión $(-1, 0)$ es trasladado al origen $(0, 0)$. En estas nuevas coordenadas la ecuación será

$$E \,:\, y^2 = x(x^2 - 3x + 3).$$

Si $\mathcal{O}$ denota el punto en E al infinito. Es obvio que el grupo de puntos racionales $E(\mathbb{Q})$ de esta nueva curva elíptica es isomorfo al grupo de puntos racionales de D.

En este caso la curva E' está definida por la ecuación

$$E' \,:\, y^2 = x(x^2 + 6x - 3).$$

Definamos el mapeo $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/{\mathbb{Q}^*}^2$ por

$$\alpha(\mathcal{O}) = 1 \pmod{{\mathbb{Q}^*}^2},$$

$$\alpha(0, 0) = b \pmod{{\mathbb{Q}^*}^2},$$

$$\alpha(x, y) = x \pmod{{\mathbb{Q}^*}^2} \text{ si } x \neq 0.$$

El mapeo α es un homomorfismo de grupos. Se demuestra que el kernel de α es igual a la imagen de $\psi(E'(\mathbb{Q}))$. Por lo tanto, α induce un homomorfismo inyectivo

$$E(\mathbb{Q})/\psi(E'(\mathbb{Q})) \hookrightarrow \mathbb{Q}^*/{\mathbb{Q}^*}^2$$

Definimos el mapeo $\overline{\alpha} : E'(\mathbb{Q}) \to {\mathbb{Q}^*}^2$ en la misma forma.

Por lo tanto la imagen de α es isomorfa a $E(\mathbb{Q})/\psi(E'(\mathbb{Q}))$. Luego, el índice $[E(\mathbb{Q}) : \psi(E'(\mathbb{Q}))]$ es igual a $|\alpha(E(\mathbb{Q}))|$. Similarmente, se tiene $[E'(\mathbb{Q}) : \varphi(E(\mathbb{Q}))] = |\overline{\alpha}(E'(\mathbb{Q}))|$.

Obsérvese que el grupo cociente $E(\mathbb{Q})/2E(\mathbb{Q})$ de acuerdo al Teorema de Mordell–Weil es de la forma

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r \oplus T/2T \cong (\mathbb{Z}/2\mathbb{Z})^r \oplus T[2],$$

donde $T[2]$ es la parte de 2–torsión de T. Por lo tanto,

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = 2^r \cdot |T[2]|. \tag{2}$$

Para un punto de 2–torsión (x, y) tenemos $y = 0$, así $x(x^2 - 3x + 3) = 0$ y la única solución racional es $x = 0$. Como $\mathcal{O}$ también es un punto de 2–torsión, tenemos $|T[2]| = 2$.

De la teoría de grupos se sigue que

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = \\ = [E(\mathbb{Q}) : \psi(E'(\mathbb{Q}))] \cdot [\psi(E'(\mathbb{Q})) : \psi \circ \varphi(E(\mathbb{Q}))]$$

$$= \frac{[E(\mathbb{Q}) : \psi(E'(\mathbb{Q}))] \cdot [E'(\mathbb{Q}) : \varphi(E(\mathbb{Q}))]}{[\ker(\psi) : \ker(\psi) \cap \varphi(E(\mathbb{Q}))]}. \quad (3)$$

Sabemos que $\ker(\psi) = \{\overline{\mathcal{O}}, (\overline{0}, \overline{0})\}$. Pero necesitamos saber cuando $(\overline{0}, \overline{0})$ es un elemento de $\varphi(E(\mathbb{Q}))$. El punto $(\overline{0}, \overline{0})$ es un elemento de $\varphi(E(\mathbb{Q}))$ si y sólo si existe un punto racional (x, y) en E con $x \neq 0$ y $y = 0$. Veremos que no existe tal punto y, por lo tanto,

$$[\ker(\psi) : \ker(\psi) \cap \varphi(E(\mathbb{Q}))] = 2.$$

De (2) y (3) obtenemos las igualdades

$$2^r = \frac{[E(\mathbb{Q}) : 2E(\mathbb{Q})]}{4} = \frac{|\alpha(E(\mathbb{Q}))| \cdot |\overline{\alpha}(E'(\mathbb{Q}))|}{4}. \quad (4)$$

Así calculando el número de elementos en las imágenes de α y $\overline{\alpha}$ es suficiente.

Veamos cómo son estas imágenes. Para determinar la imagen de α, hallaremos cuales números racionales, módulo cuadrados, pueden ocurrir como la coordenada x de puntos en $E(\mathbb{Q})$. Escribimos

$$x = \frac{m}{e^2} \quad y \quad y = \frac{n}{e^3}$$

en su expresión reducida, con $e > 0$. Si $m = 0$, entonces $(x, y) = (0, 0)$ y $\alpha(0, 0) = 3$. Veamos los puntos con m y n distintos de cero. Estos puntos satisfacen

$$n^2 = m(m^2 - 3me^2 + 3e^4). \quad (5)$$

Sea $b_1 = \text{mcd}(m, b)$, seleccionamos el signo de tal forma que $mb_1 > 0$. Entonces $m = b_1 m_1$ y $b = b_1 b_2$, con $\text{mcd}(m_1, b_2) = 1$ y $m_1 > 0$. Si sustituimos éstos en (5), concluimos que b_1 divide a n, así $n = b_1 n_1$. Así

$$n_1^2 = m_1(b_1 m_1^2 - 3m_1 e^2 + b_2 e^4).$$

Como $\text{mcd}(b_2, m_1) = 1$ y $\text{mcd}(e, m_1) = 1$, ambos factores del lado derecho son cuadrados. Por lo tanto, factorizando $n_1 = MN$, tenemos que $M^2 = m_1$ y $N^2 = b_1 m_1^2 - 3m_1 e^2 + b_2 e^4$; de donde

$$N^2 = b_1 M^4 - 3M^2 e^2 + b_2 e^4. \quad (6)$$

Por lo tanto, el punto (x, y) con el que comenzamos puede escribirse como $\left(\frac{b_1 M^2}{e^2}, \frac{b_1 MN}{e^3}\right)$, módulo cuadrados, la coordenada x es un divisor de b, luego divide a 3.

Demostraremos que el número de elementos en $\alpha(E(\mathbb{Q}))$ es igual a 2. Como $b = 3$, debemos tener cuidado con los divisores ± 1 y ± 3. De aquí en adelante diremos que el número s es un elemento de la imagen de α; entendiendo por esto la clase en $\mathbb{Q}^*/\mathbb{Q}^{*^2}$ a la cual s pertenece, es un elemento de la imagen de α. Tenemos que $1 \in \alpha(E(\mathbb{Q}))$, dado que $\alpha(\mathcal{O}) = 1$. Como $\alpha(0, 0) = b = 3$, 3 está en la imagen de α. La imagen de α es un subgrupo de $\mathbb{Q}^*/\mathbb{Q}^{*^2}$, si -1 está en la imagen de α, entonces -3 también está en ésta, y viceversa. Por lo tanto, sólo debemos tratar con uno de ellos. Tomemos $b_1 = -1$. La ecuación que obtenemos es

$$N^2 = -M^4 - 3M^2 e^2 - 3e^4. \quad (7)$$

Tomando esta ecuación módulo 3, vemos que no existe solución, ya que $\text{mcd}(M, N) = 1$. Por lo tanto, -1 no está en la imagen de α. De esto se sigue que $|\alpha(E(\mathbb{Q}))| = 2$, que es lo que queríamos demostrar.

Similarmente, podemos demostrar que el número de elementos en la imagen de $\overline{\alpha}$ es igual a 2. De la ecuación (4) se sigue que el rango de E es cero. Dado que el rango de E es cero, todos los puntos racionales en E tienen orden finito. Para calcular los puntos racionales usaremos el Teorema de Nagell–Lutz.

En este caso tenemos $\Delta = -27$, así todos los puntos racionales en E tienen $y = 0$ ó $y^2 | -27$, donde y es un entero. Tratando con todos los valores posibles de y hallamos los siguientes puntos en D: $(-1, 0)$, $(0, 1)$, $(0, -1)$, $(2, 3)$ y $(2, -3)$. Por lo tanto, el grupo $D(\mathbb{Q})$ tiene orden 6 y consiste de

$$\{(-1, 0), (0, 1), (0, -1), (2, 3), (2, -3), \mathcal{O}\}.$$

□

3.3. Demostración de Euler

Debiera ser obvio que Euler no usó la teoría de curvas elípticas. Él dió una prueba elemental, usando el método de Fermat de descenso infinito. Como ambas demostraciones usan algún tipo de descenso, esperaríamos que éstos fueran esencialmente el mismo. Daremos la demostración original de Euler y la explicaremos usando la teoría de curvas elípticas. Con esto veremos que ambas demostraciones son "esencialmente la misma".

La formulación del teorema dada por Euler es:

Teorema 3.5.
Nullus cubus, ne quidem numeris fractis exceptis, unitate auctus quadratum efficere potest praeter unicum casum, quo cubus est 8.

En otras palabras: si sumamos 1 al cubo de un racional, entonces esta suma nunca será un cuadrado, al menos que el cubo sea 8. Euler obviamente supone que los números que él considera no son iguales a cero.

Demostración:
Propositio ergo huc redit, ut $\frac{a^3}{b^3} + 1$ *nunquam esse possit quadratum praeter casum, quo* $\frac{a}{b} = 2$. *Quocirca demonstrandum erit hanc formulam* $a^3 b + b^4$ *nunquam fieri posse quadratum, nisi sit* $a = 2b$.

Desglosando, considere la ecuación $y^2 = x^3 + 1$. Suponga que esta ecuación tiene una solución racional positiva $\left(\frac{a}{b}, y\right)$, con a y b primos relativos. Esto es equivalente a decir que $\frac{a^3}{b^3} + 1$ es un cuadrado, lo cual implica que $a^3 b + b^4$ sea un cuadrado. Nótese que esta suposición ya excluye a tres de los puntos racionales hallados en la demostración anterior, a saber los puntos $(0, 1)$, $(0 - 1)$ y $(-1, 0)$. Necesitamos demostrar que $a = 2b$ da la única solución no trivial.

Haec autem expressio resolvitur in istos tres factores $b(a + b)(aa - ab + bb)$, *qui primo quadratum constituere possunt, si esse posset* $b(a + b) = aa - ab + bb$, *unde prodit* $a = 2b$, *qui erit casus, quem excepimus. Pono autem, ut ulterius pergam,* $a + b = c$ *seu* $a = c - b$, *qua facta substitutione habebitur*

$$bc(cc - 3bc + 3bb),$$

quam demonstrandum est quadratum esse non posse, nisi sit $c = 3b$; *sunt autem* b *et* c *numeri inter se primi. Hic autem duo occurrunt casus considerandi, prout* c *vel multiplum est ternarii vel secus; illo*

enim casu factores c et cc−3bc+3bb communem divisorem habebunt 3, hoc vero omnes tres inter se erunt primi.

La expresión $a^3b + b^4$ es igual a $b(a+b)(a^2 - ab + b^2)$. Este es un cuadrado si $b(a+b) = a^2 - ab + b^2$, lo cual da la solución $a = 2b$. Euler ahora aplica el mismo cambio de coordenadas que en la demostración anterior: introduce la nueva variable c, definida por $c = a + b$. Esto es equivalente a una transformación tal que $(0,0)$ sea un punto racional de 2–torsión. Aquí se tiene que $\text{mcd}(b,c) = 1$. Entonces tenemos la ecuación

$$\frac{c}{b}\left(\left(\frac{c}{b}\right)^2 - 3\frac{c}{b} + 3\right) = y^2$$

de donde vemos que el punto $P = \left(\frac{c}{b}, y\right)$ es un punto racional en la curva elíptica $y^2 = x(x^2 - 3x + 3)$, la cual llamaremos E en el resto de la demostración. Esto es equivalente a decir que

$$bc(c^2 - 3bc + 3b^2) \tag{8}$$

es el cuadrado de un número racional, como Euler dijo. Note que la solución $a = 2b$ corresponde a $c = 3b$.

De aquí en adelante Euler supone que $\frac{a}{b}$ es distinto de 2, que es equivalente a suponer que c es distinto de $3b$. Como b y c son primos relativos, el único caso en el cual los dos factores en la expresión (8) tienen un factor común mayor que 1, es cuando c y $c^2 - 3bc + 3b^2$ no son primos relativos. Esto implica que c es divisible por 3. Por lo tanto, Euler considera los casos cuando c no es múltiplo de 3 y c es un múltiplo de 3.

Caso 1: 3 no divide a c

Sit primo c non divisibile per 3; necesse erit, ut singuli illi tres factores sint quadrata, scilicet b et c et cc − 3bc + 3bb seorsim. Fiat ergo cc − 3bc + 3bb = $\left(\frac{m}{n}b - c\right)^2$; erit

$$\frac{b}{c} = \frac{3nn - 2mn}{3nn - mm} \quad vel \quad \frac{b}{c} = \frac{2mn - 3nn}{mm - 3nn},$$

cuius fractionis termini erunt primi inter se, nisi m sit multiplum ternarii.

Como 3 no divide a c, entonces b, c y $c^2 - 3bc + 3b^2$ son primos relativos y ellos deben ser cuadrados. Así $c^2 - 3bc + 3b^2 = \left(\frac{m}{n}b - c\right)^2$, donde se pueden tomar m y n primos relativos y positivos. Como $\frac{b}{c} \neq 0$, se tiene

$$\frac{b}{c} = \frac{3n^2 - 2mn}{3n^2 - m^2}.$$

Los números $3n^2 - 2mn$ y $3n^2 - m^2$ son primos relativos, a menos que 3 divida a m. Así se deben de considerar dos casos.

Caso 1.1: 3 no divide a m

Sit ergo m per 3 non divisibile; erit vel c = 3nn − mm vel c = mm − 3nn et vel b = 3nn − 2mn vel b = 2mn − 3nn. At cum 3nn − mm quadratum esse nequeat, ponatur c = mm − 3nn, quod quadratum fiat radicis m − $\frac{p}{q}$n, hincque oritur $\frac{m}{n} = \frac{3qq + pp}{2pq}$ atque

$$\frac{b}{nn} = \frac{2m}{n} - 3 = \frac{3qq - 3pq + pp}{pq}.$$

Quadratum ergo esset haec formula pq(3qq−3pq+pp), quae omnino similis est propositae bc(3bb − 3bc + cc) et ex multo minoribus numeris constat.

Suponga que 3 no divide a m. Entonces tenemos que $b = 3n^2 - 2mn$ y $c = 3n^2 - m^2$, ó $b = 2mn - 3n^2$ y $c = m^2 - 3n^2$. Tomando $3n^2 - m^2$ módulo 4, éste no puede ser un cuadrado. Por lo tanto, $c = m^2 - 3n^2$ y $b = 2mn - 3n^2$. Así $m^2 - 3n^2 = \left(m - \frac{p}{q}n\right)^2$, donde p y q son primos relativos y positivos. Entonces $\frac{m}{n} = \frac{3q^2 + p^2}{2pq}$, de donde se tiene que $\frac{b}{n^2} = \frac{3q^2 - 3pq + p^2}{pq}$. Como b es un cuadrado, entonces $\frac{3q^2 - 3pq + p^2}{pq}$ es un cuadrado y por lo tanto $pq(3q^2 - 3pq + p^2)$ también lo es. Euler procede diciendo que ha hallado enteros p y q tales que $pq(p^2 - 3pq + 3q^2)$ es un cuadrado, cuando $c^2 - 3bc + 3b^2$ lo es. Sin embargo, p y q son más pequeños, esto no fue especificado por Euler, pero obtendremos esto.

Traslademos este argumento al lenguaje de curvas elípticas. Podemos ver que estos enteros, p y q, dan un punto racional $\left(\frac{p}{q}, y'\right) = P'$ en la curva elíptica E. Veremos cual es el significado de esta reducción. Así como cuando usamos un 2–descendente en la demostración anterior, esperaríamos que esto tenga algo que ver con multiplicación por 2. Esto resultará ser verdadero. Calculando la coordenada x del punto $2P'$ obtenemos la expresión:

$$x_{(2P')} = \frac{((\frac{p}{q})^2 - 3)^2}{4y'^2} = \frac{p^4 - 6p^2q^2 + 9q^4}{4(p^3q - 3p^2q^2 + 3pq^3)}. \tag{9}$$

Calculamos $\frac{c}{b}$ en términos de p y q:

$$\frac{c}{b} = \frac{m^2 - 3n^2}{2mn - 3n^2} =$$
$$= \frac{(3q^2 + p^2)^2 - 3(2pq)^2}{2(3q^2 + p^2)(2pq) - 3(2pq)^2} = \frac{9q^4 - 6p^2q^2 + p^4}{4(p^3q - 3p^2q^2 + 3pq^3)},$$

la cual es igual a la expresión (9). Por lo tanto, hemos hallado un nuevo punto P', tal que $2P'$ es igual al punto P con el cual empezamos. Nótese la similitud de la ecuación $P = 2P'$ con la expresión $P - Q_i = 2P'$. Esto no demuestra que no existan otros puntos racionales positivos, ya que podría pasar que posteriormente llegáramos a un punto que ya tuviéramos. Ahora tenemos el problema de determinar en qué sentido los números enteros se hacen "más pequeños". En la demostración con curvas elípticas usamos alguna noción del tamaño de los puntos en una curva elíptica; a saber, la altura de un punto. Veremos si esta noción del tamaño es suficiente para el objetivo de Euler.

Veamos las alturas de los puntos en cuestión. La altura de $P = \left(\frac{c}{b}, y\right)$ es igual a $\max\{|b|, |c|\}$ y la altura de $P' = \left(\frac{p}{q}, y'\right)$ es igual a $\max\{|p|, |q|\}$. Demostraremos que la altura de P' es menor que la altura de P. Tenemos que $b = 2mn - 3n^2$, así n divide a b, lo cual implica que $|n| \leq |b|$. Además, $n = 2pq$ ó $n = pq$; por lo tanto, $|p|$ y $|q|$ son menores o iguales que $|n|$. Ahora probaremos que $\max\{|p|, |q|\}$ es menor o igual que $|b|$. Nótese que $\max\{|p|, |q|\}$ es igual a $|b|$ cuando $b = n = \max\{|p|, |q|\}$, esto pasa cuando $b = 2mn - 3n^2 = n$, así $m = 2$ y $n = 1$. Esto pasa sólo cuando $b = 1$ y $c = 1$, lo cual implica que $a = 0$, pero esto lo habíamos

excluido inicialmente. De esto se concluye que para todos los puntos racionales positivos P la altura de P' es menor que la altura de P.

Así, concluimos que si existe un punto $P = \left(\frac{c}{b}, y\right)$ en E como arriba, entonces existe una sucesión $P', P'', P''', \ldots$ de puntos en E tal que la altura de cada punto es menor que la altura de su antecesor. Pero esto es imposible, puesto que el punto P con el que empezamos tiene altura finita $\max\{|b|, |c|\}$ y todas las alturas son enteros mayores que cero. Por lo tanto, tal punto no existe.

Caso 1.2: 3 divide a m

At sit m multiplum ternarii, puta $m = 3k$; erit $\frac{b}{c} = \frac{nn - 2kn}{nn - 3kk}$, unde erit vel $c = nn - 3kk$ vel $c = 3kk - nn$; quia autem $3kk - nn$ quadratum esse nequit, ponatur $c = nn - 3kk$ eiusque radix $n - \frac{p}{q}k$, unde fiet $\frac{n}{k} = \frac{3qq + pp}{2pq}$ seu $\frac{k}{n} = \frac{2pq}{3qq + pp}$ atque

$$\frac{b}{nn} = 1 - \frac{2k}{n} = \frac{pp + 3qq - 4pq}{3qq + pp}.$$

Quadratum ergo esse deberet $(pp + 3qq)(p - q)(p - 3q)$. Ponatur $p - q = t$ et $p - 3q = u$; erit $q = \frac{t - u}{2}$ et $p = \frac{3t - u}{2}$ illaque formula abit in hanc $tu(3tt - 3tu + uu)$, quae iterum similis est priori $bc(3bb - 3bc + cc)$.

Como 3 divide a m, $m = 3k$. Entonces tenemos que

$$\frac{b}{c} = \frac{n^2 - 2kn}{n^2 - 3k^2},$$

de donde se tiene $c = n^2 - 3k^2$ y $b = n^2 - 2kn$. Como c es un cuadrado, sea $c = \left(n - \frac{p}{q}k\right)^2$ con p y q primos relativos y positivos. Entonces $\frac{n}{k} = \frac{3q^2 + p^2}{2pq}$ y, por lo tanto, $\frac{b}{n^2} = \frac{p^2 + 3q^2 - 4pq}{3q^2 + p^2}$. Como b es un cuadrado, $\frac{p^2 + 3q^2 - 4pq}{3q^2 + p^2}$ también lo es y, por lo tanto, $(p^2 + 3q^2)(p - q)(p - 3q)$ es un cuadrado. Haciendo las sustituciones $t = p - q$ y $u = p - 3q$ obtenemos la siguiente expresión:

$$tu(3t^2 - 3tu + u^2)$$

que es un cuadrado.

Euler procede en la misma forma que en el caso anterior. Afirma que ha hallado nuevos enteros t y u, tales que la expresión $tu(3t^2 - 3tu + u^2)$ es un cuadrado, además los enteros t y u son en algún sentido menores que b y c.

En términos de la teoría de curvas elípticas, hemos hallado un segundo punto racional $P' = \left(\frac{u}{t}, y'\right)$ en E. ¿Será $2P'$ igual a P?. Calculando la coordenada x del punto $2P'$ se tiene

$$x_{(2P')} = \frac{((\frac{u}{t})^2 - 3)^2}{4y'^2} = \frac{u^4 - 6u^2t^2 + 9t^4}{4(u^3t - 3u^2t^2 + 3ut^3)}. \qquad (10)$$

Calculamos $\frac{c}{b}$ en términos de t y u:

$$\frac{c}{b} = \frac{n^2 - 3k^2}{n^2 - 2kn}$$

$$= \frac{(3(\frac{t-u}{2})^2 + (\frac{3t-u}{2})^2)^2 - 12(\frac{3t-u}{2} \cdot \frac{t-u}{2})^2}{(3(\frac{t-u}{2})^2 + (\frac{3t-u}{2})^2)^2 - 2(3(\frac{t-u}{2})^2 + (\frac{3t-u}{2})^2)^2 \cdot 2\frac{t-u}{2} \cdot \frac{3t-u}{2}}$$

$$= \frac{9t^4 - 6t^2u^2 + u^4}{4tu(3t^2 - 3tu + u^2)}, \qquad (11)$$

la cual es igual a (10).

Ahora demostraremos que la altura de P' es menor que la altura de P. La sustituciones $p - q = t$ y $p - 3q = u$ son equivalentes a decir que $q = \frac{t - u}{2}$ y $p = \frac{3t - u}{2}$. Tenemos dos posibilidades: que t y u sean ambos positivos ó negativos.

(i) Supongamos que t y u son ambos positivos: Nótese que n divide a b, por lo tanto $n \leq b$; de $q = \frac{t - u}{2} > 0$ se tiene que $t > u$; tenemos $p = \frac{3t - u}{2} > \frac{3t - t}{2} = t$. Así hemos probado que $u < t < p < n \leq b$ y, por lo tanto, la altura de $P' = \left(\frac{u}{t}, y''\right)$ es menor que la altura del punto original P.

(ii) En el caso en que t y u son ambos negativos: Tenemos $q - p = |u|$ y $3q - p = |t|$, por lo tanto, $q = \frac{|t| - |u|}{2}$, y así $|t| > |u|$. Por otra parte, tenemos $\frac{n}{k} = \frac{3q^2 + p^2}{2pq}$. Note que el único divisor común posible de $3q^2 + p^2$ y $2pq$ es 2, puesto que m y n son primos relativos. Así se tiene la desigualdad:

$$n \geq \frac{3q^2 + p^2}{2} = \frac{3(|t|^2 - 2|t||u| + |u|^2) + |t|^2|t||u| + 9|u|^2}{8}$$

$$= \frac{|t|^2 - 3|t||u| + 3|u|^2}{2} > \frac{|t|^2}{2} \geq |t|. \qquad (12)$$

La última desigualdad se tiene porque t y u son enteros tales que $|t| > |u| > 0$; por lo tanto $|t| \geq 2$. Así, tenemos que $|u| < |t| < n \leq b$, y en consecuencia la altura del nuevo punto $P' = \left(\frac{u}{t}, y'\right)$ es menor que la altura del punto original $P = \left(\frac{c}{b}, y\right)$. De esto obtenemos una contradicción. Luego, el punto $P = \left(\frac{c}{b}, y\right)$ no existe.

Caso 2: 3 divide a c

Restat ergo posterior casus, quo est c multiplum ternarii, puta $c = 3d$, atque quadratum esse debet $bd(bb - 3bd + 3dd)$; quae cum iterum similis sit priori, manifestum est utroque casu evenire non posse, ut formula proposita sit quadratum. Quamobrem praeter cubum 8 alius ne in fractis quidem datur, qui cum unitate faciat quadratum. Q.E.D.

Si 3 divide a c, entonces $c = 3d$ con d un entero positivo. Como $\frac{c}{b}$ es distinto de 3, d es distinto de b. Dado que $bc(c^2 - 3bc + 3b^2)$ es un cuadrado, entonces $bd(b^2 - 3bd + 3d^2)$ también lo. Tenemos el nuevo punto $P' = \left(\frac{b}{d}, y'\right)$ en E. Como b y c son primos relativos, 3 no divide a b. Repitiendo el argumento del caso 1 para este punto, obtenemos una contradicción. Luego, el punto con el que comenzamos en este caso no existe.

En términos de curvas elípticas, lo que Euler dice es que si el punto racional $P = \left(\frac{c}{b}, y\right)$ está en E, entonces el punto $P' = P + (0, 0) = \left(3\frac{b}{c}, y'\right) = \left(\frac{3b}{3d}, y'\right) = \left(\frac{b}{d}, y'\right)$ también está en E. Pero por el caso 1 aplicado al punto P', éste no existe y, por lo tanto, el punto con el que comenzamos no existe. Compare la ecuación $P + (0, 0) = P - (0, 0) = 2P'$ con la expresión $P - Q_i = 2P'$.

En esta parte de la demostración usamos el hecho de que $\frac{c}{b} \neq 3$,

si hubiéramos aplicado el argumento anterior a $\frac{c}{b} = 3$, hubiéramos hallado el punto $\left(\frac{b}{d}, y'\right) = (1, 0)$, al cual el argumento del caso 1 no es aplicable. Este punto corresponde a las soluciones $(2, 3)$ y $(2, -3)$ en la curva elíptica original D. □

Si comparamos las demostraciones de Euler y la dada en términos de curvas elípticas, vemos que son muy parecidas, pero existe una pequeña diferencia. En la demostración de Euler, empezamos con un punto racional en E con ciertas restricciones sobre éste, por ejemplo, éste no debe ser $(1, 0)$, y usando el método de descenso infinito se concluye que no existe. En la demostración con curvas elípticas empezamos con cualquier punto racional en E, y usando el método de 2–descendente hallamos que tal punto siempre está generado por un número finito de puntos.

Los métodos de descenso producen lo mismo. Si comparamos el proceso de escribir un punto racional P en E como $P - Q_i = 2P'$ con lo hecho en la demostración de Euler, vemos que Euler hace exactamente lo mismo: en el caso 1.1 y 1.2 escribe el punto P con el que empieza en la forma $P = 2P'$, donde P' es un punto racional en E con altura menor que la altura de P. En el caso 2, primero suma el punto $(0, 0)$ al punto y luego aplica el caso 1. En términos de la expresión $P - Q_i = 2P'$, esto es equivalente a decir que $(0, 0)$ es un representante de la clase de $2E(\mathbb{Q})$ y que $P - (0, 0) = 2P'$ para algún punto racional P' en E con altura menor que la altura de $P - (0, 0)$.

Por lo tanto, podemos concluir que la forma en que Euler demuestra el Teorema 3.1 es esencialmente la misma que la demostración con curvas elípticas. Así, vemos que las sustituciones ingeniosas de Euler tienen un significado geométrico.

3.4. Demostración en Anillos

Para finalizar, damos la tercera demostración basada en la teoría de anillos; en particular usamos algunas propiedades del anillo $\mathbb{Z}[\sqrt[3]{2}]$. En particular, el grupo de unidades de este anillo está generado por -1 y $\sqrt[3]{2} - 1$, es decir, tiene rango dos.

Definición 3.3.
Para cada $x \in \mathbb{Z}[\sqrt[3]{2}]$ existen $a, b, c \in \mathbb{Z}$ únicos tales que $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$. El coeficiente c se llama el $\sqrt[3]{4}$–coeficiente de x.

Proposición 3.1.
Sea η la unidad $\sqrt[3]{2} - 1$. Los únicos exponentes $n \in \mathbb{Z}$ para los cuales η^n tiene $\sqrt[3]{4}$–coeficiente cero, son $n = 0$ y $n = 1$.

Demostración:
Sea $\pi = 1 + \sqrt[3]{2}$. Este número genera el único ideal primo que está sobre 3 en el anillo $\mathbb{Z}[\sqrt[3]{2}]$. Como $\pi^3 = (1 + \sqrt[3]{2})^3$ está en $3\mathbb{Z}[\sqrt[3]{2}]$, luego las potencias π^k y por lo tanto el $\sqrt[3]{4}$–coeficiente de π^k están en $3^{\llbracket \frac{k}{3} \rrbracket}\mathbb{Z}[\sqrt[3]{2}]$ para todo $k \geq 0$.

El $\sqrt[3]{4}$–coeficiente de $\eta = \sqrt[3]{2} - 1 = -2 + \pi$ se anula si y sólo si el correspondiente a $-\frac{\eta}{2} = 1 - \frac{\pi}{2}$ se anula. Para cada $n \in \mathbb{Z}$ tenemos que

$$\left(-\frac{\eta}{2}\right)^n = \sum_{k=0}^{\infty} \binom{n}{k} \left(-\frac{\pi}{2}\right)^k.$$

Esta serie converge π–ádicamente. Tiene sólo un número finito de términos cuando $n \geq 0$. Observamos los $\sqrt[3]{4}$–coeficientes de los términos de la serie. La serie de estos converge al $\sqrt[3]{4}$–coeficiente de η^n. El $\sqrt[3]{4}$–coeficiente de los términos con $k = 0$ y $k = 1$ es cero. Supongamos que $n \neq 0$ ó 1 y dividamos todo por $n(n-1)$, con esto tenemos

$$0 = \sum_{k=2}^{\infty} \frac{1}{k(k-1)} \binom{n-2}{k-2} (-\tfrac{1}{2})^k, \qquad \sqrt[3]{4}\text{–coeficiente de } \pi^k.$$

Como el $\sqrt[3]{4}$–coeficiente de π^k está en $3^{\llbracket \frac{k}{3} \rrbracket}\mathbb{Z}[\sqrt[3]{2}]$, y para $k \geq 5$ la valuación 3–ádica de $k(k-1)$ es estrictamente menor que $\llbracket k/3 \rrbracket$, todos los términos con $k \geq 5$ son congruentes con 0 módulo 3. Como el $\sqrt[3]{4}$–coeficiente de π^2, π^3 y π^4 es igual a 1, 3 y 6, respectivamente, tenemos que

$$\begin{aligned} 0 &\equiv \frac{1}{2}(-\tfrac{1}{2})^2 + \frac{1}{2\cdot 3}(n-2)(-\tfrac{1}{2})^3 3 + \\ &\quad + \frac{1}{3\cdot 4}\frac{(n-2)(n-3)}{2}(-\tfrac{1}{2})^4 6 \pmod 3 \\ &\equiv -1 - (n+1) + (n+1)n \equiv n^2 + 1 \pmod 3 \end{aligned}$$

lo cual no es posible. □

Proposición 3.2.
Las únicas soluciones $x, y \in \mathbb{Z}$, distintas de cero, de la ecuación diofántica

$$x^2 - y^3 = 1$$

son dadas por $(x, y) = (\pm 3, 2)$. En particular, las únicas soluciones no triviales $x, y \in \mathbb{Z}$ a la ecuación de Catalan con exponentes $p = 2$ y $q = 3$ están dadas por $(x, y) = (\pm 3, 2)$.

Demostración:
Tenemos

$$(x-1)(x+1) = y^3.$$

Si x es par, los factores de la izquierda son primos relativos. Por lo tanto $x + 1 = u^3$ y $x - 1 = v^3$ para ciertos $u, v \in \mathbb{Z}$. De donde $u^3 - v^3 = 2$. Esto implica que $u = 1$, $v = -1$ y, por lo tanto, $x = 0$; lo que da una solución trivial. Por lo tanto, x es impar. Cambiando el signo si es necesario, podemos suponer que $x \equiv 1 \pmod 4$. Entonces tenemos

$$\frac{x-1}{4} \cdot \frac{x+1}{2} = \left(\frac{y}{2}\right)^3.$$

Los factores de la izquierda son primos relativos y tenemos

$$\frac{x-1}{4} = u^3 \quad \text{y} \quad \frac{x+1}{2} = v^3, \quad \text{para algunos} \quad u, v \in \mathbb{Z}.$$

Esto implica que

$$v^3 - 2u^3 = 1.$$

En otras palabras, el número $\varepsilon = v - u\sqrt[3]{2}$ es una unidad en el anillo $\mathbb{Z}[\sqrt[3]{2}]$. Más aún, tiene norma 1. Como η tiene norma 1, entonces $\varepsilon = \eta^n$. Por otra parte, tenemos que el $\sqrt[3]{4}$–coeficiente de ε es cero, luego por la Proposición 3.1 se tiene que:

$$v - u\sqrt[3]{2} = 1 \quad \text{ó} \quad v - u\sqrt[3]{2} = \sqrt[3]{2} - 1.$$

En el primer caso tenemos $u = 0$, $v = 1$ y, por lo tanto, $y = 0$; lo que da una solución trivial. En el segundo caso, tenemos $u = v = -1$ y $x = -3$, $y = 2$. □

Nota

extraída de una carta enviada al editor por el Sr. E. Catalan, Profesor de la escuela Politécnica de París.

Le ruego, Señor, anunciar, en su colección, el teorema siguiente,que considero verdadero, aunque todavía no haya conseguido demostrarlo completamente: otros estarán más felices tal vez:

Dos números enteros consecutivos, otros que 8 y 9, no pueden ser potencias exactas; es decir: la ecuación $x^m - y^n = 1$, en la cual las incógnitas son números enteros positivos, admite sólo una solución.

El autor agradece los comentarios y observaciones del árbitro que ayudaron a mejorarlo.

Bibliografía

[1] Yann Bugeaud and Guillaume Hanrot. *Un nouveau critère pour l'équation de Catalan.*
Mathematika, **47** (2000), 63–73.

[2] J.W.S. Cassels. *On the equation* $a^x - b^y = 1$.
American Journal of Mathematics, **75** (1953), 159–162.

[3] J.W.S. Cassels. *On the equation* $a^x - b^y = 1$ *II.*
Proceedings of the Cambridge Philosophical Society, **56** (1960), 97–103.

[4] E. Catalan. *Note extraite dúne lettre adressée à l'éditeur.*
Journal für die reine und angewandte Mathematik, **27** (1844), 192.

[5] Eugène-Charles Catalan. *Quelques théorèmes empiriques. (1842–43).*
En Mélanges Mathématiques, Mémoires de la Société Royale des Sciences de Liège,
deuxième série, **12** (1885), 42–43.

[6] E.Z. Chein. *A note on the equation* $x^2 = y^q + 1$.
Proceedings of the American Mathematical Society, **56** (1976), 83–84.

[7] Leonard Eugene Dickson. History of the Theory of Numbers, volume II.
Chelsea Publishing Company, New York, 1952.

[8] L. Euler. *Commentationes Arithmeticae I.*
Opera Omnia, Series I, volume II, pages 56–58. B.G. Teubner, Basel, 1915.

[9] Chao Ko. *On the diophantine equation* $x^2 = y^n + 1,\ xy \neq 0$.
Scientia Sinica, **14** (1965), 457–460.

[10] V.A. Lebesgue. *Sur límpossibilité, en nombres entiers, de l'équation* $x^m = y^2 + 1$.
Nouvelles annales de mathématiques, **9** (1850), 178–181.

[11] Wm. J. LeVeque. *On the equation* $a^x - b^y = 1$.
American Journal of Mathematics, **74** (1952), 325–331.

[12] A. Mąkowski. *Three consecutive integers cannot be powers.*
Colloquium Mathematicum, IX (1962), 297.

[13] Preda Mihăilescu. *A Class Number Free Criterion for Catalan's Conjecture.*
J. Number Theory, **99** (2003), 225–231.

[14] Preda Mihăilescu. *Primary cyclotomic units and a proof of Catalan Conjecture.*
J. Reine Angew, **572** (2004), 167–195.

[15] Paulo Ribenboim. *Catalan's Conjecture.*
Academic Press, Boston, 1994.

[16] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves.*
Springer-Verlag, New York, 1992.

[17] Francisco Thaine. *On the ideal class groups of real abelian number fields.*
Annals of Mathematics, **128** (1988), 1–18.

[18] R. Tijdeman. *On the equation of Catalan.*
Acta Arithmetica, **29** (1976), 197–209.

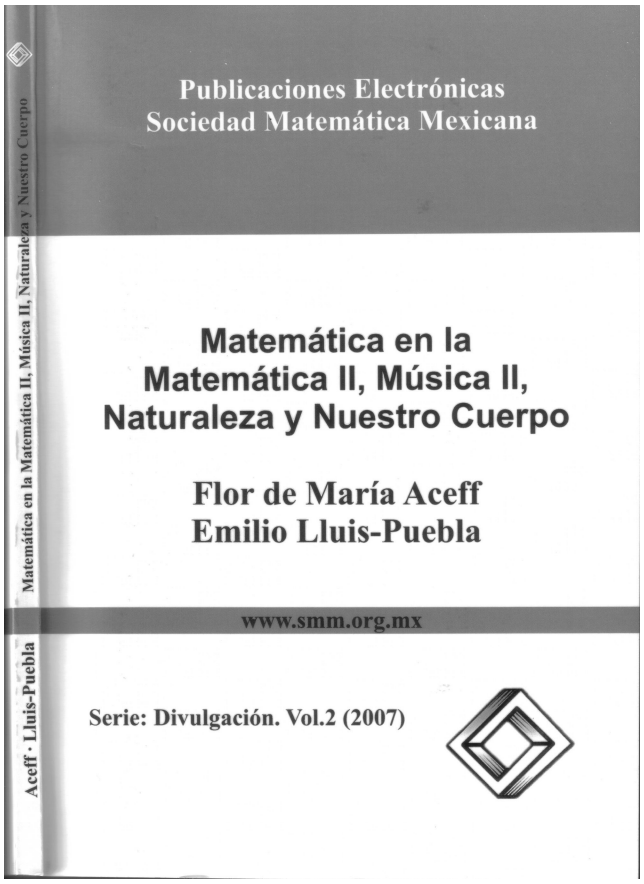
[19] Lawrence C. Washington. *Introduction to Cyclotomic Fields.*
Springer-Verlag, New York, 1982.

Matemática
en la
Matemática II, Música II,
Naturaleza y Nuestro Cuerpo.

Flor de María Aceff y Emilio Lluis-Puebla.

Publicaciones Electrónicas. Serie: Divulgación. Vol. 2. (2007)
Sociedad Matemática Mexicana.

ISBN: 968-9161-23-7 (versión en línea), 968-9161-21-0 (versión en papel), 968-9161-22-9 (versión en CD)



Este segundo volumen, al igual que el primero, tiene como propósito el de servir como motivación y orientación vocacional a los jóvenes deseosos de dedicarse a una de las aventuras más formidables del Ser Humano, la Matemática. También está dedicado a toda persona que desee obtener un concepto más aproximado acerca de la Matemática y sus practicantes. Está dirigido tanto para un público en general como para un lector de nivel matemático diverso. Hemos tratado de dejarle algo a cada uno de ellos.

En "Matemática y matemáticos II" se escribe acerca de la Matemática, sus características, la investigación y progreso en ella. Como ejemplo del surgimiento de una teoría matemática se presenta la K-Teoría Algebraica. También, como matemática aplicada se hace lo correspondiente con la Teoría Matemática de la Música. Finalmente, se exponen pensamientos acerca de la Computación y su relación con la Matemática.

Con respecto a "Matemática en la Música II", actualmente es perceptible que en las últimas dos décadas del siglo pasado (y hasta la fecha) hubo una gran tendencia en la Matemática de realizar no sólo aplicaciones sino hacer Matemática en una gran variedad de campos del conocimiento, y el campo de la Música no ha sido la excepción.

Uno de los propósitos de la Teoría Matemática de la Música es la de establecer un marco conceptual estable, definiendo los conceptos en una forma precisa. Se expone el acercamiento de Mazzola para muchos problemas musicales el cual está basado en la Teoría de Topos. Se introduce el concepto de Denotador el cual permite describir los objetos musicales y se mencionan las ideas detrás del mismo. Se concluye que estamos actualmente viviendo un cambio tan radical en la Musicología como el que se experimentó en la Física hace 500 años.

Muchos patrones de la naturaleza son tan irregulares y fragmentados que exhiben varios niveles de complejidad vistos con la geometría usual. La existencia de estos patrones nos reta a estudiar esas formas que con la geometría usual parecen no tener forma, es decir, a investigar la morfología de lo "amorfo". En el capítulo III presentamos los fractales, que son la herramienta para estudiar los patrones complejos de la naturaleza.

Con respecto a “Matemática en Nuestro Cuerpo”, los fractales son estructuras geométricas que se pueden usar para analizar muchas estructuras biológicas que no son explicables con análisis convencionales. Aquí se exhibe el análisis fractal y se muestra cómo se puede aplicar al análisis del hueso trabecular, a la estructura del árbol bronquial y al análisis de las arritmias cardiacas.

Hemos decidido incluir este segundo texto dentro de las Publicaciones Electrónicas de la Sociedad Matemática Mexicana con el ánimo de predicar con el ejemplo y mostrar la confianza que tenemos en este tipo de publicación.

Las Publicaciones Electrónicas de la Sociedad Matemática Mexicana constituyen una biblioteca de libre acceso para toda la comunidad matemática del país y del mundo. Consta de cuatro series: Textos, Memorias, Divulgación y Cursos.

Los libros son de libre acceso en línea pero también pueden adquirirse por solicitud en dos versiones: en papel con cubierta plastificada y en CD.

La serie Textos consta de dos tipos de libros: por un lado, libros de texto nuevos escritos expresamente para este medio y por otro, libros que han sido utilizados por generaciones durante años y que terminaron su venta por otras casas editoras.

La serie Memorias deja establecido por escrito los trabajos presentados en las diversas reuniones matemáticas, en especial donde la Sociedad Matemática Mexicana tiene presencia.

La serie Divulgación consiste de una colección de libros para motivar a niños, jóvenes y adultos a estudiar y apreciar la Matemática y su comunidad. También incluye libros de difusión de la Matemática de todos los niveles para estudiantes y profesores de Matemática.

La serie Cursos desea presentar diversos cursos que se hayan realizado en los Congresos de la Sociedad u otras reuniones.

Es de hacer notar que las Publicaciones Electrónicas de la Sociedad Matemática Mexicana no le generan ningún gasto a nuestra Sociedad. Son autosuficientes y proporcionan un servicio a la comunidad (matemática en particular) de todo el mundo.

La Sociedad Matemática Mexicana conjuntamente con la generosidad de los autores ofrecen un regalo a la comunidad matemática y público en general, de cualquier parte del planeta, el cual contribuye a la formación de la cultura científica. Basta con que el lector se conecte a la página en internet de la Sociedad Matemática Mexicana www.smm.org.mx y acceda a las Publicaciones Electrónicas..

Flor de María Aceff
Emilio Lluis-Puebla

Departamento de Matemática
Facultad de Ciencias
Universidad Nacional Autónoma de México
fmas@hp.fciencias.unam.mx
lluisp@servidor.unam.mx

Semblanza del **Prof. Enrique Valle Flores** por Oscar Mario Rodríguez

Reconocimiento al Profr. Enrique Valle Flores en la ceremonia de develación de la placa que formaliza el nombre Auditorio “Mat. Enrique Valle Flores”, del Departamento de Matemáticas, Universidad de Sonora.

Hablar o escribir sobre una persona puede resultar una tarea difícil, pero referirse a un personaje conocido y tan estimado resulta más ambicioso que fácil, porque se agolpan los recuerdos, se asoma la emoción y se presenta la tentación de desbordar las anécdotas.

El Profesor Valle Flores nació en Fresnillo, Zacatecas el 18 de Abril de 1916. Como la mayoría de sus contemporáneos inició la carrera de Ingeniería, que era lo común antes de que se contara con una carrera de Matemáticas. Formó parte de ese pléyade que inició la aventura de realizar y fomentar una formación en matemáticas y en ciencias, entre los que destacan: José Adem Chaim, Rodolfo Morales, Félix Recillas Juárez, Carlos Graef Fernández, Guillermo Haro, Samuel Gitler, Carlos Imaz, Sotero Prieto, Manuel Sandoval Vallarta, Alfonso Nápoles Gándara, Nabor Carrillo Flores, quien fue ingeniero con doctorado en Matemáticas; rector de la UNAM en la época del cambio de los edificios del centro de la ciudad de México a la Ciudad Universitaria y Presidente de la Sociedad Matemática Mexicana en el período en que el Congreso fue por primera vez en la Universidad de Sonora.

Inició como muchos de nosotros, tal vez por el exceso de trabajo cuando trataba de hacerse de un patrimonio para su familia, que incluso trabajó en el Colegio Militar, llegó a padecer del síndrome del Profesor, así como algunos de sus amigos.

Su tesis de licenciatura fue sobre teoría del área. Abordó muchos campos de la matemática. Con base a su manejo de la Estadística creó, con la Dra. Ana María Flores, la Dirección de Normas y Medidas de la Secretaría de Industria y Comercio.

Con la realización de la Asamblea Matemática de la Sociedad Matemática Mexicana de 1953, en la Universidad de Sonora se inició el anhelo de contar con una escuela de Ciencias. Lo que se concretó con el inicio de actividades de la Escuela de Altos Estudios el 4 de Marzo de 1964. Contaba con las Licenciaturas en Letras, en Física y en Matemáticas.

Esta escuela contó con el apoyo de la Sociedad Matemática Mexicana, el Instituto de Matemáticas de la UNAM y del CIEA del IPN. Algunos maestros, siendo profesores allá, fueron comisionados para colaborar con la Escuela de Altos Estudios. Tal es el caso de Manola Garín de Álvarez, quien era secretaria de actas de la SMM y del Profesor Enrique Valle Flores, quien era profesor titular del Instituto de Matemáticas, quién además había tenido estancias en instituciones de otros países.

El compromiso era sacar a una generación de egresados. Para ello contaron con el apoyo de egresados destacados, tanto de la UNAM como del IPN. Manola dirigió la escuela desde el período 1964-1965, siendo ella directora se realizó el Congreso de la Sociedad Matemática Mexicana en la Universidad de Sonora a principios de 1966.

El profesor Valle llegó al inicio del período 1967-1968, nos reincorporábamos a continuar la carrera, después de la huelga estudiantil de 1967. La escuela era dirigida por el Dr. en Matemáticas Oscar Valdivia.

Recalcando el compromiso que se tenía con la joven Escuela, Valle impulsó que regularmente contáramos con la visita de destacados científicos, así como estancias de otros.

Un caso especial lo constituye el Dr. José Adem Chaim (1921-1991), a quien esperábamos en Mayo, ya fuera para dictar algún curso o conferencias o para ser jurado en algún examen profesional. Adem fue un reconocido topólogo y algebrista, del que se llegó a decir que si se deseaba estudiar álgebra homológica habría que hacerlo en México con Adem. En los sesenta se le solicitó que abordara el problema de encontrar la trayectoria de retorno de la luna. En una ocasión nos comentó que prácticamente del patio de su casa salió el Granma.

Hoy, las cosas aparentemente son mas fáciles, pero recordemos que nos referimos a la época pionera, en la Universidad sólo se contaba con seis edificios escolares: Edificio principal, en donde se daban clases de varias carreras, la escuela Secundaria, que salió del campus en 1964 para dejar su edificio para la Escuela de Altos Estudios, la Escuela de Agricultura y Ganadería, que hoy forma parte de DICTUS, la Escuela de Ingeniería, la Escuela de Ciencias Químicas y la Escuela Preparatoria. Además el Gimnasio, hoy parte del Departamento de Arquitectura, y el estadio Castro Servín, con solo las graderías del oeste. En 1964, el Lic. Adolfo López Mateos inauguró dos más: uno para Contabilidad y Administración y otro para Derecho. Actualmente uno en la ECA y el otro en Economía. Además inauguró el de Ciencias Químicas y las graderías del lado este del estadio.

En una época difícil para la Escuela de Altos Estudios, y tal vez para la misma Universidad, hubo quienes se pronunciaran por el cierre de la escuela, ya que fue la única que se manifestó en contra de una política interna contraria al buen desempeño de la Universidad como una institución educativa de prestigio. (Fuimos testigos en ANUIES, de que los paquetes de solicitudes para becas enviados a la Universidad de Sonora, eran devueltos sin siquiera abrirlos).

En esas circunstancias, como expresó el Profesor Valle, lo obligamos a que se hiciera cargo de la Dirección de la Escuela.

Valle impulsó la realización de los Simposium México - Estados Unidos de Ecuaciones Diferenciales. Habiéndose realizado uno en la Universidad de Sonora, otro en la Universidad de Arizona y otro en el CIEA del IPN.

Quienes tuvimos la oportunidad de ser sus alumnos abrevamos en sus conocimientos de Algebra (superior, lineal, moderna), matemáticas puras y aplicadas, probabilidad, teoría de la medida, análisis funcional, análisis matemático, análisis complejo. Basta recordar sus exposiciones y los textos recomendados para sus cursos para aceptar de nuevo que gozábamos sus clases. Contaba con una biblioteca personal muy completa y selecta.

Es interesante leer las apreciaciones que tienen de él las personas que decidieron estudiar matemáticas gracias a sus clases, como es el caso del Dr. Gonzalo Zubieta.

Por lo general Valle fue quien nos propuso los temas de tesis a los miembros de las primeras generaciones y nos guió en el desarrollo de las mismas.

Era riguroso en el uso del lenguaje, tanto el simbólico de las matemáticas como el lenguaje común; exigía precisión en los conceptos.

A su vez realizó actividades que nos permitiera incursionar en el ámbito interinstitucional, relacionándonos con los matemáticos y físicos de otras instituciones del país y del extranjero, así como con funcionarios del CONACYT, ANUIES, UNAM, CIEA del IPN, Escuela de Agricultura de Chapingo.

Impulsados por él, desarrollamos varios seminarios en períodos vacacionales de verano en aulas de la Facultad de Ciencias de la UNAM, para los cuales tramitaba apoyo económico en instituciones de la ciudad de México.

Para acrecentar el compañerismo que reinaba en la Escuela de Altos Estudios, instituyó una cita el primer sábado de Agosto, para todos los miembros de ella e invitados que se encontraran en México.

Las personas que lo conocimos sabemos que correspondía de manera instantánea a la amistad y que siempre estaba dispuesto a brindar apoyo personal o de ser necesario, buscarlo.

Una de las realizaciones mas importantes de Valle la escuché del Maestro Jorge Ontiveros Almada: “Mira la labor de Valle me dijo, ve a nuestro amigo de la sierra, con sus botas, sus levy, su camisa de remaches, su sombrero y su cinturón vaquero planteando modelos matemáticos”.

Para nosotros no fue difícil seleccionar un padrino para nuestra generación. Así, mientras que a los egresados de Derecho, los apadrinaba el Presidente Luís Echeverría desde Nogales, nosotros contábamos con la presencia, en nuestra escuela, de nuestro flamante padrino el Profesor Enrique Valle Flores.

El otro Valle llegaba a festejar con su risa franca las bromas que hacía o que se le hacían o al narrar alguna travesura de su juventud; o cuando era testigo de algún hecho chusco, como cuando presenciamos la reacción de un asno al asustarse con su propio reflejo, o al recordarle de manera jocosa, de como “rescatamos” a Martha Mejía de Valle de una asamblea en la Preparatoria de San Ildefonso.

También resultaba ser estricto cuando la ocasión lo requería, en el uso correcto de las cosas. En cierta ocasión después de muchos minutos de observación y esperando que otro lo hiciera, le colgó el teléfono a una persona que nos lo había pedido prestado diciéndole: “disculpe joven, pero los teléfonos no son para jugar”.

En ocasiones mostraba un sarcasmo muy fino, como cuando solicitaba: “por favor cierre la puerta, no se vaya a congelar todo el mundo”. O cuando recordaba el evento familiar en “el Templo de Nuestra Señora de Concreto”.

Considero que acuñó algunas frases propias de él: Al referirse a las matemáticas lo hacía en singular, ya que consideraba que “la Matemática es única”. Cuando alguien retrasado en su trabajo le ofrecía algún bocado le contestaba: “yo devoro tesis”. En ocasiones hacía un manejo curioso del anidamiento, diciendo por ejemplo: “cada uno es mejor que todos los demás juntos”.

Pero tuvo una contundente: “jamás permitan que decida sobre su capacidad alguien que no haya demostrado la suya”.

Así mismo tenía refranes propios, algunos de nivel de postgrado, por no decir muy colorados.

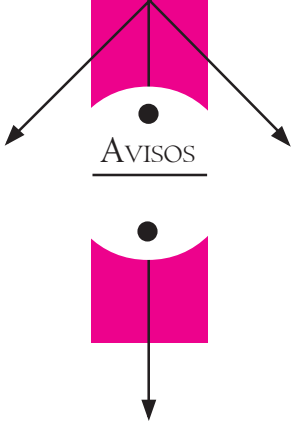
Podía llegar a sorprendernos con alguna de sus vivencias. En una ocasión, al desviarme de la ruta que traíamos, comenzó una plática de cómo había conocido, en los cuarenta, La Laguna de Beltranes, municipio de El Rosario Sinaloa. Al terminar su relato sólo le dije: “No es posible profesor, precisamente ahí es a donde vamos, es la casa de mis abuelos”.

1988 se llevó al Dr. Carlos Graef Fernández (1911-1988), amigo de Valle, ambos se trataban con mucha camaradería, estaba relacionado con la Escuela de Altos Estudios, a la que visitó en varias ocasiones, fue un reconocido físico, él le puso el nombre al ladrillo de Hilbert. Muy ameno conversador y conferencista. En una de sus conferencias manifestó su especial predilección por cierta transformación al decir: “si me aplican esta transformación me convierten en un hombre normal”.

Ese año también se llevó a nuestro estimado y de muy gratos recuerdos, Profesor Enrique Valle Flores, comprometido para siempre con la Universidad de Sonora.

Deseo terminar, transcribiendo el último párrafo de mi tesis de licenciatura:
“Quiero manifestar mi agradecimiento al Profesor Enrique Valle Flores por su dinámica paciencia y las energías gastadas en el desarrollo de las matemáticas en Sonora”.

Hermosillo Sonora; 30 de Agosto de 2007.



CARTA INFORMATIVA

SOCIEDAD MATEMÁTICA MEXICANA

Número 54,
Octubre de 2007

Publicación de la
Sociedad Matemática Mexicana, A.C.
Apartado Postal 70-450,
04510 México, D.F.
Tel. 5622-4481 / 82
Fax 5622-4479
smm@smm.org.mx

DISEÑO Y PRODUCCIÓN

S y G editores, SA de CV
Tels. 5619-5293 / 5617-5610
sygeditores@cablevision.net.mx

PORTADA

Euler

ICME 11

La décima primera edición del Congreso Internacional de Educación Matemática se realizara por primera vez en América Latina

Fechas: del 6 al 13 de Julio del 2008

La bella ciudad de Monterrey ha sigo elegida como la sede para tan importante reunión