Premio Abel 2016: Andrew J. Wiles

por

Álvaro Lozano-Robledo

In Memoriam
Francisco Javier Cilleruelo Mateo (1961 - 2016)

Resumen. La Academia de Ciencias y Letras de Noruega ha otorgado el Premio Abel de 2016 a Andrew Wiles «por su impresionante demostración del Último Teorema de Fermat mediante la conjetura de modularidad para las curvas elípticas semiestables, iniciando una nueva era en la teoría de números». En este artículo repasamos la trayectoria de Andrew Wiles quien, aparte de demostrar el último teorema de Fermat, ha atacado muchas de las grandes conjeturas de la teoría algebraica de números, tales como la conjetura de Birch y Swinnerton-Dyer, la Conjetura Central de la teoría de Iwasawa, la conjetura de Shimura-Taniyama-Weil y la conjetura de Fontaine-Mazur.

1. Prólogo

El 15 de marzo del 2016 la Academia de Ciencias y Letras de Noruega anunció que concedía el Premio Abel de este año a Andrew Wiles. Poco después, mi muro de Facebook se llenaba de enlaces y comentarios de mis colegas de Teoría de Números, y también de aquellos familiares y amigos que deciden compartir conmigo noticias matemáticas cuando, raramente, las encuentran a su paso. En estas ocasiones me tengo que preparar mentalmente para leer los artículos de prensa que se avecinan (normalmente escritos a un nivel matemático lejos del que desearía), y tras este anuncio en particular aparecieron muchas reseñas a nivel mundial: Nature, The Guardian, Time, NPR, New Scientist, Forbes, CNN, The Hindu, etc. También en España los medios se hicieron eco de la noticia: ABC, EFE, El Mundo, El País, La Vanguardia, El Faro de Vigo, etc. He de decir que en esta ocasión la mayoría de las notas de prensa eran aceptables, aunque casi todas seguían a rajatabla el mismo patrón, contando la historia del jovencito Wiles que encontró un libro sobre el «teorema» y se prometió a sí mismo resolverlo, e incluyendo la misma foto que aquí reproducimos con la pizarra de fondo (figura 1). Curiosamente, la foto tan reproducida contiene un enunciado incorrecto del último teorema, pues $x = y = z = 0$ es una solución trivial en enteros para todo $n \geq 1$.

Como no se le pueden pedir peras al olmo, me conformo con que la prensa divulgue algo de matemáticas, aunque les dé un tratamiento somero y de contenido

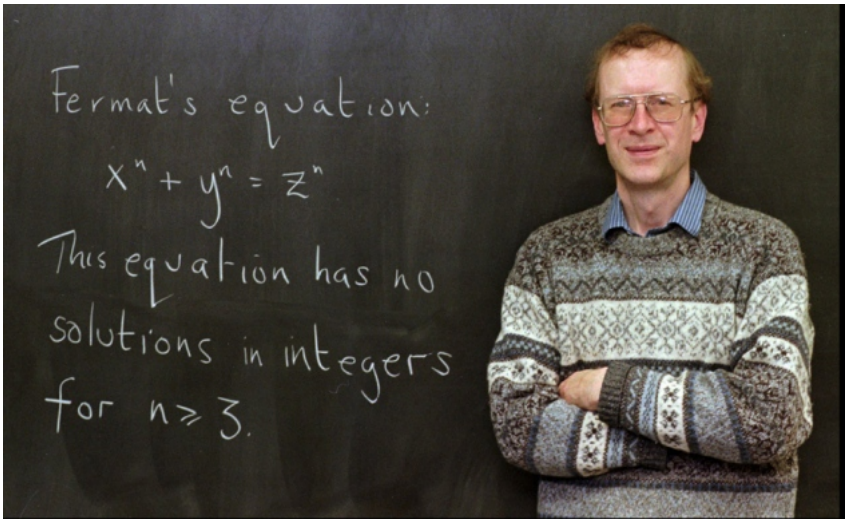


Figura 1: Andrew J. Wiles y un enunciado incorrecto del último teorema de Fermat.

muy ligero para no ahuyentar a sus lectores. Pero me sorprendía que un artículo tras otro se referiera a Wiles como ganador del premio por demostrar el último teorema de Fermat, algo que ocurrió hace 20 años, y no por el resto de sus contribuciones y su trayectoria. Al principio me parecía normal, e incluso inevitable, que la prensa se refiriera únicamente al teorema de Fermat (y la resolución de la conjetura de la modularidad, en honrosas excepciones) como la gran contribución de Wiles, pues es algo que se puede explicar en pocas líneas... pero al leer noticia tras noticia en la que se mencionaba el teorema de Fermat como el «teorema ganador» de Wiles, me fui a la página de la Academia Noruega para leer su propia nota de prensa, y cuál fue mi sorpresa al encontrar tambien allí que se le concedía el Premio Abel «por su impresionante demostración del Último Teorema de Fermat mediante la conjetura de modularidad para las curvas elípticas semiestables, iniciando una nueva era en la teoría de números». Cierto, sin duda, pero conociendo las contribuciones de Wiles, la motivación me sabe a poco. Por ejemplo, se puede comparar el texto de la Academia con los análogos referidos a Jean-Pierre Serre (Premio Abel en 2003),

> *Por su papel clave en moldear la forma moderna de muchas partes de las matemáticas, incluyendo la topología, la geometría algebraica y la teoría de números*,

o a John Tate (Premio Abel en 2010),

> *Por su impacto vasto y duradero en la teoría de números*,

los cuales me parecen justos y acertados, pues dan una idea de la profundidad de las contribuciones de estos grandes nombres de las matemáticas.

Después de pasar un par de días refunfuñando al leer más y más notas de prensa que encasillaban a Wiles con Fermat, me llegó un correo de la RSME, en el cual me

daban la oportunidad de escribir un artículo para La Gaceta acerca de Wiles. Y estas palabras que van a leer son el resultado.

Mi intención es desmarcar a Wiles del último teorema de Fermat (que relegaremos al ejemplo 6.2), y concentrarme en el resto de sus contribuciones a la teoría de números. En el siglo XX, se formularon varias conjeturas que han establecido una hoja de ruta para la investigación en la teoría (algebraica) de números, y con este artículo me propongo recalcar que Wiles ha tenido un papel excepcional en el estudio de casi todas las grandes conjeturas de esta área. Y por todas sus grandes contribuciones que vamos a destacar, el premio Abel es ciertamente merecido, incluso si la fama de Fermat no hubiera estado de por medio.

Si por otra parte el lector esperaba encontrar aquí otra historia más de cómo el joven Wiles se propuso resolver y acabó resolviendo el último teorema de Fermat, le recomendamos una de las muchísimas referencias que hay al respecto, que van desde documentales como *The Proof* (NOVA, PBS) o *Fermat's Last Theorem* (BBC Horizon), libros que son para el público en general ([1], [30]), títulos adecuados para estudiantes de grado en Matemáticas ([13], [25]), hasta el nivel de doctorado y postdoctorado ([4], [29]). De las referencias disponibles, cabe destacar el bello artículo [10] y el compendio de artículos en [9]. El autor de estas líneas ha escrito un libro ([23]) dedicado al material necesario para entender el enunciado de la conjetura de la modularidad (también conocida como la conjetura de Shimura-Taniyama-Weil), y dos artículos en La Gaceta, uno acerca de las curvas elípticas ([20]) y otro sobre el último teorema de Fermat y su conexión con la teoría de Iwasawa ([22]).

Índice de Contenidos

Este artículo está organizado en las siguiente secciones:

2. *Trayectoria y Legado de Wiles*, donde se recoge una corta biografía de Andrew Wiles, que incluye su número de publicaciones y descendientes matemáticos.
3. *Álgebra, Análisis, Geometría y Teoría de Números* contiene una breve introducción a los tipos de objetos de los que tratan las obras de Wiles. En particular, esbozamos definiciones y ejemplos de curvas elípticas, formas modulares, funciones L y representaciones de Galois.

Los títulos de las siguientes secciones se refieren a colaboraciones entre Wiles y otros autores en varias publicaciones que se conocen en los círculos de expertos precisamente por estas abreviaciones.

4. *Coates-Wiles* se refiere a un artículo entre Wiles y su director de tésis, John Coates, donde demuestran uno de los primeros casos de la conjetura de Birch y Swinnerton-Dyer (BSD). En esta sección discutimos la conjetura de BSD y el trabajo de Coates y Wiles.
5. *Mazur-Wiles* es un trabajo conjunto entre Wiles y Barry Mazur (y más tarde Wiles en solitario), en el que demuestran la Conjetura Principal de la teoría de Iwasawa. Aquí describiremos someramente la conjetura y referimos al lector a otras referencias para tratamientos más completos.

6. *Wiles y Taylor-Wiles* son los trabajos (el segundo con su estudiante Richard Taylor) en los que se demuestra, en el caso semiestable, la conjetura de Shimura-Taniyama-Weil, también conocida como conjetura de la modularidad, y que concluyeron con la demostración del último teorema de Fermat.
7. *Skinner-Wiles* es una colaboración con Christopher Skinner en la que se presentan demostraciones de ciertos casos de la conjetura de Fontaine-Mazur.

Acabamos este prólogo con un **aviso al lector**: la intención de este artículo es de divulgación y no está escrito para los expertos (que, por otra parte, ya conocen todo este material). Por tanto, nos hemos tomado libertades en simplificar definiciones y teoremas cuando los enunciados resultarían demasiado técnicos. En todo caso, hemos intentado dejar claro cuando hemos sintetizado el material, y proporcionamos referencias a otros artículos y libros donde el lector puede encontrar introducciones rigurosas a estos temas.

AGRADECIMIENTOS. Quisiera agradecer la oportunidad de escribir este artículo a los directores de LA GACETA, a Enrique González Jiménez por sus comentarios de una primera versión, y al revisor anónimo por su lectura detallada y sus comentarios y consejos. Doy también muchas gracias a Adolfo Quirós por una revisión muy minuciosa del artículo. Por último, este artículo está dedicado a Francisco Javier Cilleruelo Mateo, creador de la sección de *El Diablo de los Números* de LA GACETA, cuya ausencia deja un vacío en la teoría de números en España muy difícil de compensar.

2. TRAYECTORIA Y LEGADO DE WILES

Andrew John Wiles nace el 11 de abril de 1953 en Cambridge, Inglaterra, y estudia en la Universidad de Oxford, graduándose en 1974, año en el que comienza su doctorado bajo la dirección de John Coates.

Durante el doctorado hace una primera visita a Harvard como Benjamin Pierce Assistant Professor. Tras recibir el doctorado en 1980, y una estancia en la Universidad de Bonn, vuelve a los Estados Unidos en 1981 para trabajar en el Institute for Advanced Study de Princeton. En 1985 viaja a París con una beca Guggenheim para visitar el Institut des Hautes Études Scientifique y también la École Normale Supérieure. En 1988 regresa a Oxford y en 1989 se le nombra Fellow de la Royal Society, pero en 1990 vuelve a Princeton como profesor Eugene Higgins de Matemáticas. En 2011 se traslada de nuevo a Oxford, ahora como profesor de investigación de la Royal Society.

Wiles ha acumulado numerosos premios de gran prestigio durante su carrera: el Premio Schock de la Real Academia Sueca de las Ciencias, el Premio Fermat de la Universidad Paul Sabatier de Toulouse, el Premio Wolf de Matemáticas, el Premio de Matemáticas de la Academia Nacional de Ciencias de los Estados Unidos (al mismo tiempo que es nombrado académico extranjero), el Premio King Faisal, el *Clay Research Award*, el Premio Pitágoras y el Premio Shaw, entre otros. En 1998, superando la edad límite de los 40 años para la medalla Fields, la Union Matemática Internacional le concede una placa de plata en el Congreso Internacional

Figura 2: John Coates y su estudiante, Andrew Wiles.

de Matemáticos. En 1999, un asteroide se nombra en su honor, el ahora llamado Asteroide 9999 Wiles. En el año 2000, la Reina de Inglaterra le nombra *Knight Commander of the Order of the British Empire*, con lo que pasa a ser *Sir Andrew Wiles*.

MathSciNet recoge 26 publicaciones de Andrew Wiles entre 1977 y 2015. Destacan cinco artículos en *Annals of Mathematics*, cuatro en *Inventiones Mathematicae*, uno en PNAS (*Proc. Nat. Acad. Sci. USA*), otro en *American Journal of Mathematics*, dos en *Duke Math Journal*, uno en *Institut des Hautes Études Scientifiques*, y uno en *Compositio Mathematica*.

Según el *Mathematics Genealogy Project*, Wiles ha tenido 21 descendientes directos entre 1981 y 2012 (y 144 «nietos»), entre ellos algunos matemáticos de gran renombre, como Karl Rubin, Ehud de Shalit, Fred Diamond, Richard Taylor, Brian Conrad, Christopher Skinner o Manjul Bhargava (Medalla Fields en 2014).

3. Álgebra, Análisis, Geometría y Teoría de Números

Las contribuciones de Wiles han tenido un papel fundamental en comprender las conexiones teóricas entre cinco tipos de objetos matemáticos que, a priori, son de naturaleza muy distinta: curvas elípticas (geometría algebraica), representaciones de Galois, extensiones abelianas (álgebra y teoría de representaciones), funciones L y formas modulares (análisis complejo).

Estos objetos están relacionados con la teoría de números de una forma u otra y, sorprendentemente, entre sí (figura 3). Hoy en día, las conexiones que se empezaron a vislumbrar entre curvas elípticas y formas modulares se han generalizado a las categorías mucho más amplias de motivos y formas automorfas, en lo que se denomina *Programa de Langlands* (véase la figura 4, imagen que se puede ampliar y estudiar

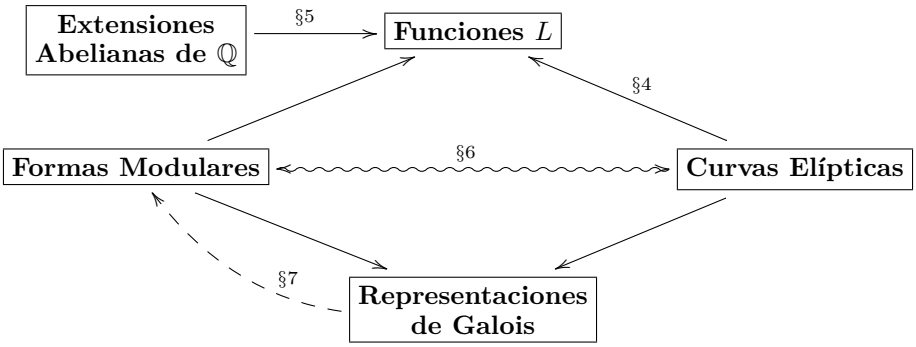


Figura 3: Las distintas conexiones entre curvas elípticas, representaciones de Galois, extensiones abelianas, funciones L y formas modulares que son estudiadas en los trabajos de Wiles (*et al.*), que exploramos en las Secciones §4, §5, §6 y §7.

en la base de datos LMFDB.org).

Describir en detalle los cinco vértices de la figura 3 nos llevaría varios volúmenes ([33], [11], [26], [7], [9]), por tanto en ésta sección nos limitaremos a esbozar definiciones de los objetos de interés con varios ejemplos concretos para ilustrar la teoría (véase también [28]).

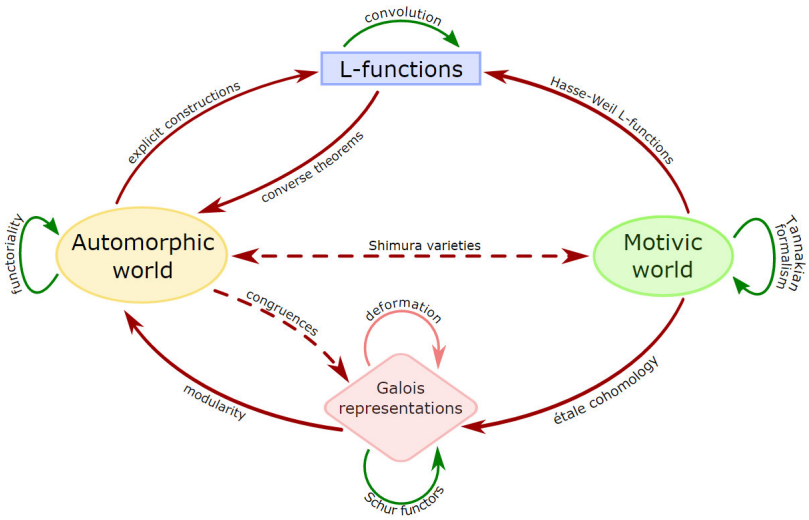


Figura 4: El mapa de ruta del *Programa de Langlands*. Este diagrama es una generalización de la figura 3, y se puede explorar en la base de datos de funciones L y formas modulares (LMFDB.org).

3.1. Curvas Elípticas

Una **curva elíptica (sobre $\mathbb{Q}$)** es una curva proyectiva, no singular, de género 1, definida por ecuaciones con coeficientes en $\mathbb{Q}$, y que tiene al menos un punto definido sobre $\mathbb{Q}$. Por ejemplo, las curvas E dadas por $y^2 = x^3 + Ax + B$, con $A, B \in \mathbb{Q}$ y $4A^3 + 27B^2 \neq 0$, son elípticas, y toda curva elíptica se puede reducir a un modelo de este tipo (que llamamos *ecuación de Weierstrass*). El requisito de tener un punto definido sobre $\mathbb{Q}$ queda satisfecho sin más que fijarnos en el único punto *en el infinito* de la curva, que es $\mathcal{O} = [0 : 1 : 0]$. Si el lector quiere profundizar, recomendamos [32], [33]. El autor ha publicado [20] en La Gaceta. Esta sección está basada en [23].

Las puntos racionales $E(\mathbb{Q})$ de E están dotados de una estructura de grupo (abeliano), para la que $\mathcal{O}$, el punto en el infinito, es el elemento neutro. La operación de grupo en los puntos de $y^2 = x^3 + Ax + B$ está definida de modo que la identidad $P + Q + R = \mathcal{O}$ se cumple si y sólo si $P, Q, R \in E(\mathbb{Q})$ están en la misma línea. El famoso teorema de Mordell-Weil nos dice que $E(\mathbb{Q})$ es un grupo abeliano finitamente generado y, por tanto, $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$ donde $E(\mathbb{Q})_{\text{tors}}$ es el subgrupo finito de elementos de torsión, y el entero $R_{E/\mathbb{Q}} \geq 0$ es el rango de $E(\mathbb{Q})$.

Ejemplo 3.1. La curva E dada por la ecuación de Weierstrass $y^2 = x^3 - 169x$ es una curva elíptica definida sobre $\mathbb{Q}$. Usando métodos como el teorema de Nagell-Lutz ([20]), podemos ver que $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0, 0), (\pm 13, 0)\}$. Sin embargo, $R_{E/\mathbb{Q}}$ es más difícil de calcular. ¿Es $R_{E/\mathbb{Q}} \geq 1$? En otras palabras, ¿es $E(\mathbb{Q})$ infinito? Responderemos a esta pregunta usando técnicas analíticas que desarollamos a lo largo del artículo. El lector impaciente puede saltar al ejemplo 6.1.

Para ilustrar cómo las curvas elípticas aparecen de manera natural al estudiar problemas de geometría y teoría de números, introducimos un problema clásico famoso (y sin resolver).

El Problema de los Números Congruentes. *Decimos que un entero $n \geq 1$ es un número congruente si existe un triángulo rectángulo cuyos lados son de longitud racional y su área es igual a n. ¿Qué números naturales son congruentes?*

Por ejemplo, el número 6 es congruente porque el triángulo de lados $(a, b, c) = (3, 4, 5)$ tiene área $\frac{3\cdot 4}{2} = 6$. El número 30 también es congruente, gracias al triángulo $(5, 12, 13)$. El número 5 es congruente ya que, aunque no hay ningún triángulo recto con lados enteros y área igual a 5, nuestra definición permite lados de longitud racional y el triángulo $\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$ tiene área 5. No permitimos triángulos de lados irracionales aunque su área sea un entero. Por ejemplo, el triángulo $(1, 2, \sqrt{5})$ tiene área 1, pero esto no dice que 1 sea un número congruente (de hecho, como veremos a continuación, el número 1 *no* es congruente).

El problema de los números congruentes es uno de los problemas más antiguos sin resolver. Desde hace más de un milenio los matemáticos han tratado de caracterizar los números congruentes. El primer registro escrito del problema data del Medievo, cuando aparece en un manuscrito árabe escrito antes del año 972. También se sabe que Johannes de Palermo, allá por el año 1220, propuso a Leonardo

Pisano, más conocido como *Fibonacci*, el problema de encontrar un triángulo rectángulo de área 5, y Fibonacci encontró el triángulo $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$. En 1225, Fibonacci escribió un tratado más general sobre el problema de los números congruentes, en el que afirmaba (sin prueba) que si n es un cuadrado perfecto, entonces n no es congruente. La demostración de este teorema tuvo que esperar hasta que Pierre de Fermat (1601-1665) demostró que el número 1, y por tanto todo cuadrado, no es un número congruente (curiosamente, su demostración puede usarse para demostrar el caso $n = 4$ del último teorema de Fermat).

La conexión entre los números congruentes y las curvas elípticas viene dada por la siguiente biyección. Sea $n > 0$ y definamos conjuntos

$$C_n = \{(a,b,c) : a^2 + b^2 = c^2,\ \frac{ab}{2} = n\},\ E_n = \{(x,y) : y^2 = x^3 - n^2 x,\ y \neq 0\}.$$

Entonces, existe una biyección $f : C_n \to E_n$ dada por

$$f((a,b,c)) = \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right),\ f^{-1}((x,y)) = \left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right).$$

El lector puede fácilmente demostrar que f es una biyección. Por ejemplo, la curva $E : y^2 = x^3 - 25x$ tiene un punto racional $(-4, 6)$ que corresponde al triángulo $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$. Pero E tiene otros puntos, como $(\frac{1681}{144}, \frac{62279}{1728})$ que corresponde al triángulo

$$\left(\frac{1519}{492}, \frac{4920}{1519}, \frac{3344161}{747348}\right)$$

que también tiene área 5. Véase la Figura 5.

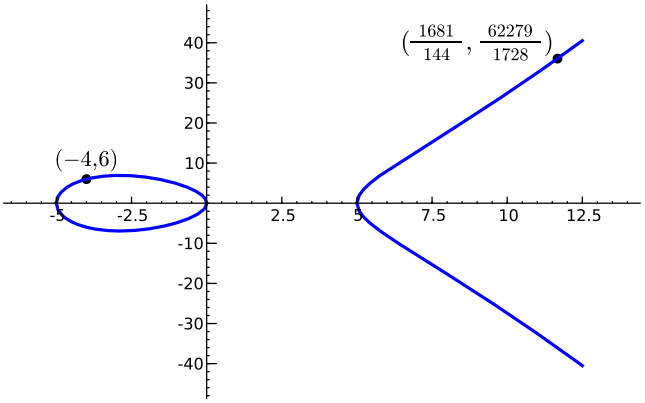


Figura 5: Dos puntos racionales en la curva elíptica $y^2 = x^3 - 25x$.

A día de hoy, no tenemos una respuesta completa al problema de los números congruentes, pero se han demostrado varios resultados parciales y algunos resultados fuertes que dependen de otras conjeturas (BSD) y que describiremos en la Sección 3.3. Por ahora, proponemos las siguientes preguntas al lector.

Pregunta 3.2. *¿Son* 2, 13 *o* 157 *números congruentes? Gracias a la biyección* $C_n \to E_n$*, nuestra cuestión es equivalente a preguntar si existen puntos en* $E_2(\mathbb{Q})$*,* $E_{13}(\mathbb{Q})$ *y* $E_{157}(\mathbb{Q})$ *con* $y \neq 0$*.*

Una historia más completa del problema de los números congruentes se puede leer en [12], C. XVI. En el libro [18] se trata el problema desde un punto de vista moderno, mientras que en [37], Sección 6.5.3, el punto de vista es computacional (usando Sage). Otro artículo de interés es [8].

3.2. Formas Modulares

Las formas modulares son las formas diferenciales holomorfas de ciertas superficies de Riemann, llamadas *curvas modulares*. La curva modular más sencilla se obtiene como cociente del semiplano superior complejo, $\mathbb{H} = \{a + bi : b > 0\}$, por una relación de equivalencia dada por transformaciones racionales de $\mathbb{C}$:

$$z \sim z' \text{ si y solo si } z' = \frac{az+b}{cz+d}, \text{ donde } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}).$$

El cociente $Y(1) = \mathbb{H}/\mathrm{SL}(2,\mathbb{Z})$ (véase la figura 6) es una superficie de Riemann, pero no es compacta. Para compactificarla es necesario añadir un punto *en el infinito*, llamado una «cúspide». El resultado, $X(1) = Y(1) \cup \{\infty\}$, es isomorfo a la recta proyectiva $\mathbb{P}^1(\mathbb{C})$.

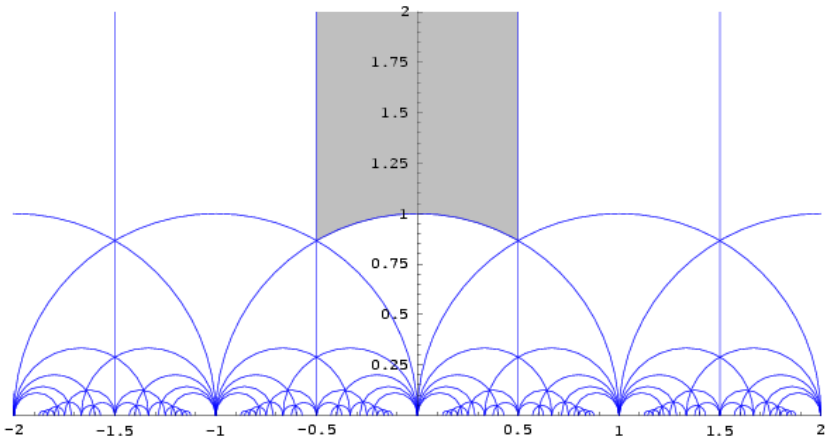


Figura 6: Cada región es un conjunto completo de clases de equivalencia de la acción de $\mathrm{SL}(2,\mathbb{Z})$ sobre $\mathbb{H}$. Por ejemplo, la región (infinita) en gris se puede indentificar con la superficie $Y(1)$.

En general, si Γ es un subgrupo de $\mathrm{SL}(2,\mathbb{Z})$ que cumple ciertas condiciones de congruencia, podemos definir una superficie de Riemann $Y(\Gamma)$ y su correspondiente compactificación $X(\Gamma)$. Por su relación con las curvas elípticas, destacamos los

subgrupos $\Gamma_0(N)$, para cada $N \geq 1$, definidos por

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : c \equiv 0 \text{ mód } N \right\}$$

y las curvas modulares correspondientes, $X_0(N) = X(\Gamma_0(N))$, que son el resultado de compactificar el cociente $Y_0(N) = \mathbb{H}/\Gamma_0(N)$. Los puntos en la diferencia $X_0(N) \setminus Y_0(N)$ se denominan las *cúspides* de $X_0(N)$.

Ahora podemos definir con más precisión las formas modulares (para $\Gamma_0(N)$): una **forma modular de peso k y nivel** N es una k-forma diferencial holomorfa de $X_0(N)$. De manera equivalente, podemos definir una forma modular (de peso k y nivel N) como una función $f : \mathbb{H} \to \mathbb{C} \cup \{\infty\}$ que es holomorfa y además cumple que

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

para cualquier $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ (en este caso, $f(z)dz$ es la k-forma diferencial de la primera definición). Una *forma cuspidal* es una forma modular $f(z)$ tal que $f(c) = 0$ para toda cúspide c de $X_0(N)$.

Como es el caso con las curvas elípticas, las formas modulares aparecen de forma natural en problemas de teoría de números y también en otras areas de las matemáticas (e.g., la reciente resolución del problema de empaquetamiento de esferas en dimensión 8 [40] y dimensión 24 [6]).

EJEMPLO 3.3. Ramanujan (en 1916) estaba interesado en la expansión del producto $\prod_{n\geq 1}(1-x^n)^{24}$, el cual, en lenguaje moderno, define una forma modular de gran importancia: la función $\Delta(z) = (2\pi)^{12}\prod_{n\geq 1}(1-q^n)^{24}$, donde $q = e^{2\pi iz}$, es una forma modular de peso $k = 12$ para $\mathrm{SL}(2,\mathbb{Z})$. Si escribimos $\Delta(z) = (2\pi)^{12}\sum_{n\geq 1}\tau(n)q^n$, los coeficientes $\tau(n)$ vienen dados por la función τ de Ramanujan, cuyos valores son el tema de varias de sus famosas conjeturas.

EJEMPLO 3.4. El conjunto $M_k(N)$ de todas las formas modulares de peso k y nivel N es un espacio vectorial complejo de dimensión finita. Por ejemplo, cuando $N = 5408$, la dimensión de $M_2(5408)$ es 748. El conjunto $S_2(5408)$ de las formas cuspidales de peso 2 y nivel 5408 es un subespacio vectorial de dimensión 673 de $M_2(5408)$. Por ejemplo, existe una forma modular cuspidal $f(z)$ en $S_2(5408)$ que tiene la siguiente expansión de Fourier:

$$f(z) = q + 2q^5 - 3q^9 + 2q^{17} - q^{25} - 10q^{29} + 2q^{37} - 10q^{41} - 6q^{45} - 7q^{49} + 14q^{53} + O(q^{60}),$$

donde $q = e^{2\pi iz}$ como antes. Esta forma modular se denomina una *newform* porque es un autovector para todos los *operadores lineales de Hecke* y es también autovector para otros operadores que actúan sobre el espacio de formas modulares (y que no espeficicaremos aquí para simplificar la discusión). En el espacio $S_2(5408)$ hay 47 formas que son del tipo *newform*.

Para profundizar en los temas de curvas modulares y formas modulares, recomendamos [11] y [36].

3.3. Funciones L

Una **función** L es una función $L(s)$ que viene dada por una serie de la forma

$$L(s) = \sum_{n=1}^{\infty} a_n n^{-s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = a_1 + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \cdots$$

con coeficientes $a_n \in \mathbb{C}$. Las funciones L que discutimos en este artículo convergen para todos los números complejos s en algún semiplano $\Re s > C$ y, en muchos casos, $L(s)$ tiene una continuación analítica o meromorfa a todo el plano complejo. En teoría de números nos interesan las funciones L porque estos objetos analíticos revelan información algebraica que, irónicamente, es difícil de encontrar con métodos algebraicos.

Ejemplo 3.5. La función zeta de Riemann, $\zeta(s)$, es la función L más famosa:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots .$$

Algunos de los valores de la función ζ son bien conocidos. Por ejemplo, el valor $\zeta(2) = \sum \frac{1}{n^2} = \pi^2/6$ se puede calcular con análisis de Fourier y la identidad de Parseval. La conexión entre $\zeta(s)$ y la teoría de números proviene de la identidad que llamamos un *producto de Euler*:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \frac{1}{1-p^{-s}} = \left(\frac{1}{1-2^{-s}}\right) \cdot \left(\frac{1}{1-3^{-s}}\right) \cdot \left(\frac{1}{1-5^{-s}}\right) \cdots .$$

Riemann fue pionero en explotar la relación entre los zeros de $\zeta(s)$ y la distribución de los números primos dentro de los números naturales.

Ejemplo 3.6. Dirichlet demostró su teorema de la infinitud de primos en progresiones aritméticas (i.e., si $a, N \in \mathbb{Z}$ son primos entre sí, entonces hay infinitos primos $p \equiv a$ mód N) usando un tipo de funciónes L que hoy en día denominamos *funciones L de Dirichlet*, y que definimos a continuación.

Sea $N > 0$ y sea $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ un carácter de Dirichlet (un homomorfismo de grupos[1]), que extendemos a una función $\chi : \mathbb{Z} \to \mathbb{C}$ con $\chi(a) = \chi(a \text{ mód } N)$ si $\text{mcd}(a, N) = 1$ y $\chi(a) = 0$ cuando $\text{mcd}(a, N) > 1$. Entonces, definimos la función L de Dirichlet asociada a χ como

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Por ejemplo, cuando $\chi = \chi_0$ es el carácter de Dirichlet trivial, entonces $L(s, \chi_0) = \zeta(s)$ es la función zeta de Riemann. Igual que $\zeta(s)$, las funciones L de Dirichlet también tienen productos de Euler:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p} \frac{1}{1 - \chi(p)p^{-s}}.$$

[1]Dado un anillo A, denotaremos por $A^\times$ el grupo multiplicativo de las unidades de A.

Figura 7: Johann Peter Gustav Lejeune Dirichlet (1805-1859) y Georg Friedrich Bernhard Riemann (1826-1866).

EJEMPLO 3.7. Sea $f(z) = \sum_{n\geq 1} a_n q^n \in S_k(N)$ una forma modular cuspidal (cómo las hemos definido en Sección 3.2). Entonces, la función L asociada a la forma $f(z)$ es, esencialmente, la transformada de Mellin de f, y viene dada por

$$L(f,s) = \sum_{n\geq 1} a_n n^{-s} = a_1 + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \cdots$$

Hecke demostró que si $f(z)$ es una forma modular cuspidal de peso par k y nivel N, y $f(z)$ es un autovector para los operadores T_p de Hecke, con $T_p(f) = a_p \cdot f$, para todo primo $p \geq 2$, entonces $L(f,s)$ tiene un producto de Euler:

$$L(f,s) = \prod_{p|N} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{k-1-2s}}.$$

Por ejemplo, la forma modular de peso 2 y nivel 5408 del ejemplo 3.4 dada por

$$f(z) = q+2q^5-3q^9+2q^{17}-q^{25}-10q^{29}+2q^{37}-10q^{41}-6q^{45}-7q^{49}+14q^{53}+O(q^{60}),$$

tiene función L con expansión de Fourier

$$L(f,s) = 1+\frac{2}{5^s}-\frac{3}{9^s}+\frac{2}{17^s}-\frac{1}{25^s}-\frac{10}{29^s}+\frac{2}{37^s}-\frac{10}{41^s}-\frac{6}{45^s}-\frac{7}{49^s}+\frac{14}{53^s}+\cdots$$

Como $f(z)$ es una *newform* de $S_2(5408)$, en particular es un autovector para todo T_p, y por tanto $L(f,s)$ tiene un producto de Euler

$$\begin{aligned} L(f,s) \quad = \quad & \left(\frac{1}{1+3^{1-2s}}\right)\cdot\left(\frac{1}{1-2\cdot 5^{-s}+5^{1-2s}}\right)\cdot\left(\frac{1}{1+7^{1-2s}}\right)\cdot\left(\frac{1}{1+11^{1-2s}}\right)\cdot \\ & \left(\frac{1}{1-2\cdot 17^{-s}+17^{1-2s}}\right)\cdot\left(\frac{1}{1+19^{1-2s}}\right)\cdot\left(\frac{1}{1+23^{1-2s}}\right)\cdot \\ & \left(\frac{1}{1+10\cdot 29^{-s}+29^{1-2s}}\right)\cdot\left(\frac{1}{1+31^{1-2s}}\right)\cdot\left(\frac{1}{1-2\cdot 37^{-s}+37^{1-2s}}\right)\cdots, \end{aligned}$$

donde hemos utilizado que $N = 5408 = 2^5 13^2$, $a_p = 0$ para $p = 2, 3, 7, 11, 13, 19, 23, 31$, y $a_5 = a_{17} = a_{37} = 2$, $a_{29} = -10$, etc.

Ejemplo 3.8. Sea E una curva elíptica sobre $\mathbb{Q}$ dada por una ecuación de Weierstrass[2] $y^2 = x^3 + Ax + B$ con coeficientes $A, B \in \mathbb{Z}$. Para cada número primo p podemos considerar la reducción de E sobre el cuerpo finito $\mathbb{F}_p$ y contar el número de puntos N_p de $E(\mathbb{F}_p)$. Aunque la curva $E/\mathbb{Q}$ no es singular, la curva $E/\mathbb{F}_p$ puede ser singular. Si $E/\mathbb{F}_p$ no es singular decimos que E tiene buena reducción en p. Si por el contrario $E/\mathbb{F}_p$ es singular, entonces decimos que E tiene mala reducción multiplicativa (hay dos tipos, *split* y *non-split*[3]) o aditiva, dependiendo de si la singularidad es un nodo (e.g., $y^2 \equiv x(x-1)^2$ mód p para $p > 2$) o una cúspide (e.g., $y^2 \equiv x^3$ mód p), respectivamente. Decimos que una curva elíptica es *semiestable* si tiene buena reducción o reducción multiplicativa para todo primo p.

Sea $a_p = p + 1 - N_p = p + 1 - \#E(\mathbb{F}_p)$. Definimos el factor local de E en p como

$$L_p(T) = \begin{cases} 1 - a_p T + pT^2, \text{ si } E \text{ tiene buena reducción en } p, \\ 1 - T, \text{ si } E \text{ tiene reducción multiplicativa } \textit{split} \text{ en } p, \\ 1 + T, \text{ si } E \text{ tiene reducción multiplicativa } \textit{non-split} \text{ en } p, \\ 1, \text{ si } E \text{ tiene reducción aditiva en } p. \end{cases}$$

Finalmente, definimos la *función L de Hasse-Weil de E* como el producto de Euler

$$L(E, s) = \prod_p \frac{1}{L_p(p^{-s})}.$$

Por ejemplo, sea $E : y^2 = x^3 - 169x$. Esta curva elíptica tiene mala reducción aditiva en $p = 2$ y 13, y buena reducción para todo primo $p \neq 2, 13$ (por tanto, esta curva no es semiestable). La siguiente tabla contiene los valores N_p y $a_p = p + 1 - \#E(\mathbb{F}_p)$ para todos los primos $p \leq 53$:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
N_p	3	4	4	8	12	14	16	20	24	40	32	36	52	44	48	40
a_p	0	0	2	0	0	0	2	0	0	-10	0	2	-10	0	0	14

Por tanto, la función L de Hasse-Weil asociada a E tiene el producto de Euler

$$\begin{aligned} L(E, s) \quad = \quad & \left(\frac{1}{1 + 3^{1-2s}}\right) \cdot \left(\frac{1}{1 - 2 \cdot 5^{-s} + 5^{1-2s}}\right) \cdot \left(\frac{1}{1 + 7^{1-2s}}\right) \cdot \left(\frac{1}{1 + 11^{1-2s}}\right) \cdot \\ & \left(\frac{1}{1 - 2 \cdot 17^{-s} + 17^{1-2s}}\right) \cdot \left(\frac{1}{1 + 19^{1-2s}}\right) \cdot \left(\frac{1}{1 + 23^{1-2s}}\right) \cdot \\ & \left(\frac{1}{1 + 10 \cdot 29^{-s} + 29^{1-2s}}\right) \cdot \left(\frac{1}{1 + 31^{1-2s}}\right) \cdot \left(\frac{1}{1 - 2 \cdot 37^{-s} + 37^{1-2s}}\right) \cdots \end{aligned}$$

y si desarrollamos el producto, obtenemos una serie

$$L(E, s) = 1 + \frac{2}{5^s} - \frac{3}{9^s} + \frac{2}{17^s} - \frac{1}{25^s} - \frac{10}{29^s} + \frac{2}{37^s} - \frac{10}{41^s} - \frac{6}{45^s} - \frac{7}{49^s} + \frac{14}{53^s} + \cdots$$

[2] Técnicamente la ecuación debe ser *minimal*, pero no entraremos a definir este concepto.

[3] Podríamos traducirlo como *escindidas* y *no escindidas*, pero suelen usarse los términos ingleses.

que, *curiosamente*, coincide con los primeros términos de la función L asociada a la forma modular cuspidal de peso 2 y nivel 5408 que hemos descrito en los ejemplos 3.4 y 3.7. Exploraremos esta conexión (la *modularidad* de E) en la Sección 6.

3.4. Representaciones de Galois

La teoría de números algebraica estudia las propiedades de los cuerpos de números, esto es, las extensiones finitas de $\mathbb{Q}$. Si fijamos una clausura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$, toda esta información viene empaquetada en el *grupo absoluto de Galois de* $\mathbb{Q}$, denotado por $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, que se puede definir como el límite inverso

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K/\mathbb{Q}),$$

donde el límite es sobre todas las extensiones finitas K de $\mathbb{Q}$ dentro de la clausura fijada $\overline{\mathbb{Q}}$. Esta construcción como límite inverso de grupos finitos dota a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ de una topología profinita. Un método para estudiar la estructura de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ es la teoría de representaciones. Sea R un anillo (normalmente $\mathbb{Z}/n\mathbb{Z}$, los enteros p-ádicos $\mathbb{Z}_p$, anillos de polinomios, etc.) dotado de una topología de grupo, y sea $n \geq 1$. Una *representación (lineal) de Galois* es un homomorfismo de grupos $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(n, R)$ que es continuo con respecto la topología profinita de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ y la topología de R. Para profundizar en representaciones de Galois recomendamos el capítulo VIII de [9] y el capítulo *Deformations of Galois representations* de [7].

EJEMPLO 3.9. Sea p un primo y sea $\mu_{p^n} \subset \overline{\mathbb{Q}}$ el conjunto de todas las raíces de la unidad cuyo orden divide a p^n, es decir, $\mu_{p^n} = \{\zeta_{p^n}^m : 0 \leq m < p^n\}$ donde $\zeta_{p^n} = e^{2\pi i/p^n}$. El grupo $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permuta los elementos de μ_{p^n} e induce una representación de Galois

$$\chi_{p^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(1, \mathbb{Z}/p^n\mathbb{Z}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$$

definida por $\chi_{p^n}(\sigma) = m$ tal que $\sigma(\zeta_{p^n}) = \zeta_{p^n}^m$. La representación χ_{p^n} se llama el *carácter ciclotómico modulo* p^n. Si formamos el límite inverso (variando n) de todas las p^n-raíces de la unidad $T_p(\mu) = \varprojlim \mu_{p^n}$, entonces $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ también actúa sobre $T_p(\mu)$ y los caracteres ciclotómicos producen una representación

$$\chi_{p^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(1, \mathbb{Z}_p) \cong \mathbb{Z}_p^\times.$$

donde $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ es el anillo de los enteros p-ádicos y $\mathbb{Z}_p^\times$ son las unidades de $\mathbb{Z}_p$. La representación χ_{p^∞} se denomina el *carácter ciclotómico p-ádico*.

De gran interés son aquellas representaciones que provienen de la geometría.

EJEMPLO 3.10. Sea E una curva elíptica definida sobre $\mathbb{Q}$ y consideremos $E(\overline{\mathbb{Q}})$, los puntos de E definidos sobre $\overline{\mathbb{Q}}$. Los puntos de $E(\overline{\mathbb{Q}})$ gozan de una estructura de grupo abeliano y podemos definir el subgrupo de puntos cuyo orden divide a p^n, normalmente denotado por $E[p^n] \subset E(\overline{\mathbb{Q}})$, al que llamamos *subgrupo de p^n-torsión* de E. El grupo absoluto de Galois actúa sobre $E[p^n]$ permutando los puntos e induce una representación

$$\rho_{E,p^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p^n]).$$

Si consideramos E como una curva definida sobre $\mathbb{C}$, entonces se sabe que $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, donde Λ es un retículo de $\mathbb{C}$ (un subgrupo aditivo discreto tal que $L \otimes \mathbb{R} = \mathbb{C}$) y por tanto se deduce que $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ para todo $n \geq 2$. En particular, $\mathrm{Aut}(E[p^n]) \cong \mathrm{Aut}(\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}) \cong \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ y, tras elegir una $\mathbb{Z}/p^n\mathbb{Z}$-base de $E[p^n]$, conseguimos una representación de Galois

$$\rho_{E,p^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p^n]) \cong \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z}),$$

tal que $\det(\rho_{E,p^n}) = \chi_{p^n}$ es el carácter ciclotómico módulo p^n del ejemplo 3.9. También podemos definir el *módulo de Tate* de E como el límite inverso (variando n) $T_p(E) = \varprojlim E[p^n]$, y obtenemos una representación de Galois p-ádica 2-dimensional

$$\rho_{E,p^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_p(E)) \cong \mathrm{GL}(2, \mathbb{Z}_p),$$

cuyo determinante es el carácter ciclotómico p-ádico.

Por ejemplo, sea E la curva $y^2 = x^3 - 169x$ de los ejemplos 3.1 y 3.8. La 2-torsión de ésta curva son los puntos

$$E[2] = \{\mathcal{O}, (0,0), (13,0), (-13,0)\}.$$

Como todos los puntos de $E[2]$ están definidos sobre $\mathbb{Q}$, entonces $\rho_{E,2} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$ es la representación trivial, con $\rho_{E,2}(\sigma) = \mathrm{Id}$ para todo automorfismo $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Para todos los demás primos, se puede demostrar que la representación $\rho_{E,p}$ tiene la siguiente imagen:

$$\mathcal{N}_p = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \begin{pmatrix} a & b \\ b & -a \end{pmatrix} : a, b \in \mathbb{Z}/p\mathbb{Z},\ a^2 + b^2 \not\equiv 0 \text{ mód } p \right\} \subset \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}),$$

que es el normalizador de un grupo de Cartan de $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$. La imagen de ρ_{E,p^∞} es la versión p-ádica de $\mathcal{N}_p$, es decir

$$\mathcal{N}_{p^\infty} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \begin{pmatrix} a & b \\ b & -a \end{pmatrix} : a, b \in \mathbb{Z}_p,\ a^2 + b^2 \in \mathbb{Z}_p^\times \right\} \subset \mathrm{GL}(2, \mathbb{Z}_p).$$

Este tipo de imagen p-ádica sólo puede ocurrir cuando E tiene *multiplicación compleja o CM* (un curva con CM tiene más endomorfismos de lo normal). Cuando una curva E sobre $\mathbb{Q}$ no tiene CM, Serre demostró que la imagen de ρ_{E,p^∞} tiene índice finito en $\mathrm{GL}(2, \mathbb{Z}_p)$ para todo primo p, y la imagen es igual a $\mathrm{GL}(2, \mathbb{Z}_p)$ para todos los primos excepto un número finito de ellos. La curva $E : y^2 = x^3 - 169x$ tiene CM por $\mathbb{Z}[i]$, es decir, el grupo de endomorfismos es isomorfo a $\mathbb{Z}[i]$ (si una curva no tiene CM entonces $\mathrm{End}(E) \cong \mathbb{Z}$), donde $[n] : E \to E$, para cada $n \in \mathbb{Z}$, corresponde al endomorfismo $P \mapsto nP$ y la función $[i] : E \to E$ viene dada por $[i](x_0, y_0) = (-x_0, i \cdot y_0)$.

Ejemplo 3.11. Las representaciones de Galois asociadas a formas modulares son un tanto más complicadas de describir (véase [27] ó [11]). Sea $f(z) \in S_k(N)$, es decir, sea f una forma modular cuspidal de peso k y nivel N que supondremos, además, que es una *newform*. En particular, $f(z) = \sum_{n \geq 1} a_n q^n$ está normalizada con $a_1 = 1$ y es

un autovector para los operadores de Hecke, con $T_p(f) = a_p \cdot f$. Una consecuencia de la teoría de formas modulares es que los coeficientes a_n son algebraicos (de hecho, son *enteros algebraicos*) y además el cuerpo $K_f = \mathbb{Q}(\{a_n : n \geq 1\})$ es una extensión finita de $\mathbb{Q}$. Dada la forma f, Shimura contruyó una variedad abeliana[4] A_f definida sobre $\mathbb{Q}$, que es un cociente de la variedad jacobiana de la curva modular $X_0(N)$, de dimensión igual al grado de la extensión $K_f/\mathbb{Q}$. Como los puntos de A_f tienen una estructura de grupo, podemos definir los subgrupos de p^n-torsión $A_f[p^n]$ de A_f como en el caso de las curvas elípticas y definir representaciones de Galois

$$\rho_{f,p^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(A_f[p^n])$$

y sus versiones p-ádicas $\rho_{f,p^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(T_p(A_f))$, donde $T_p(A_f)$ es el módulo de Tate de A_f, es decir, $\varprojlim A_f[p^n]$.

Por ejemplo, si $f = \sum_{n\geq 1} a_n q^n$ es una *newform* de peso 2 y nivel N con $K_f = \mathbb{Q}(\{a_n\}) = \mathbb{Q}$, entonces la variedad abeliana A_f es de dimensión 1, es decir, una curva elíptica definida sobre $\mathbb{Q}$. Si tomamos en concreto la forma modular $f(z)$ de los ejemplos 3.4 y 3.7, entonces A_f es la curva $E_{13} : y^2 = x^3 - 169x$ (véase el ejemplo 4.4 para la notación). Por tanto, las representaciones de Galois que provienen de la forma modular f y de la curva elíptica E_{13} coinciden.

4. COATES-WILES

Coates, J.; Wiles, A. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* **39** (1977), no. 3, 223-251.

En la Sección 3 hemos presentado los elementos que forman los vértices de la figura 3 (y son ejemplos de los vértices de la figura 4, que es mucho más general). En esta sección, nos concentramos en la arista

Curvas Elípticas ⟶ **Funciones** L

y su máxima expresión que es la conjetura de Birch y Swinnerton-Dyer. Como hemos visto en la Sección 3.3, dada una curva E definida sobre $\mathbb{Q}$, podemos asociarle una función L, la función $L(E, s)$ de Hasse-Weil. En 1965, Birch y Swinnerton-Dyer conjeturaron que el comportamiento de la función $L(E, s)$ en el entorno de $s = 1$ está íntimamente relacionado con la aritmética del grupo de puntos racionales $E(\mathbb{Q})$. Recordamos al lector (Sección 3.1) que el teorema de Mordell-Weil implica que $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$, donde $R_{E/\mathbb{Q}}$ es el rango de $E(\mathbb{Q})$.

CONJETURA 4.1 (Conjetura de Birch y Swinnerton-Dyer). *Sea E una curva elíptica sobre $\mathbb{Q}$ y sea $L(E, s)$ la función L de Hasse-Weil de E. Entonces:*

[4]Las variedades abelianas son el análogo en dimensión superior de las curvas elípticas. En particular, son variedades algebraicas proyectivas lisas con una estructura de grupo.

Figura 8: Bryan Birch (izquierda) y Sir Peter Swinnerton-Dyer (derecha). Esta fotografía es cortesía de William Stein.

1. *$L(E,s)$ tiene un cero en $s=1$ de orden igual al rango $R_{E/\mathbb{Q}}$ de $E(\mathbb{Q})$. Es decir, el desarrollo de Taylor de $L(E,s)$ en $s=1$ es de la forma*

$$L(E,s) = C_0 \cdot (s-1)^{R_E} + C_1 \cdot (s-1)^{R_E+1} + C_3 \cdot (s-1)^{R_E+2} + \cdots$$

   donde C_0 es una constante no nula.

2. *El residuo de $L(E,s)$ en $s=1$, es decir, el coeficiente C_0, tiene una expresión explícita en función de invariantes de $E/\mathbb{Q}$. Más precisamente,*

$$C_0 = \lim_{s\to 1} \frac{L(E,s)}{(s-1)^{R_E}} = \frac{|Ш_E| \cdot \Omega_E \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

El lector puede leer más acerca de la conjetura de Birch y Swinnerton-Dyer (BSD) en la descripción [44] (¡escrita por Wiles!) del premio para los Problemas del Milenio propuestos por el Instituto Clay en el año 2000. La recompensa de un millón de dolares por la demostración de esta conjetura sigue en pie.

La conjetura BSD sólo se ha demostrado en algunos casos concretos, aunque recientemente Bhargava y Shankar han demostrado una estadística que implica que BSD es cierto para una proporción positiva de todas las curvas elípticas sobre $\mathbb{Q}$. El primer caso de la conjetura fue demostrado en 1977 por Coates y Wiles [5] para curvas con CM. Este es su resultado principal:

Teorema 4.2 (Coates-Wiles, 1977). *Sea E una curva elíptica sobre $\mathbb{Q}$ con CM y sea $L(E,s)$ la función L de Hasse-Weil de E. Si $E(\mathbb{Q})$ es un grupo infinito, entonces $L(E,1)=0$.*

Es decir, Coates y Wiles demuestran una dirección de la conjetura de BSD en el caso de multiplicación compleja: si el rango es mayor que cero, entonces el orden del cero de $L(E,s)$ en $s=1$ es al menos 1. La demostración está basada en la teoría

de *unidades elípticas* (el lector puede encontrar en [21] una introducción a este tipo de unidades algebraicas). Su teorema, además, se extiende a curvas definidas sobre cuerpos de números, siempre y cuando tengan multiplicación compleja por un cuerpo cuadrático imaginario de número de clases 1.

EJEMPLO 4.3. Sea E_2 la curva $y^2 = x^3 - 4x$. Esta curva tiene multiplicación compleja (sus endomorfismos tienen estructura $\mathbb{Z}[i]$, igual que toda curva $y^2 = x^3 - Dx$; véase la exposición al final del ejemplo 3.10) y el valor de $L(E_2, 1)$ es

$$L(E_2, 1) = 0{,}927037338651\ldots$$

El teorema de Coates-Wiles muestra que $E_2(\mathbb{Q})$ es finito (i.e., $R_{E_2/\mathbb{Q}} = 0$) y por tanto $E_2(\mathbb{Q}) = E_2(\mathbb{Q})_{\text{tors}}$. No es difícil calcular la torsión de esta curva y ver que

$$E_2(\mathbb{Q}) = E_2(\mathbb{Q})_{\text{tors}} = E_2[2] = \{\mathcal{O}, (0,0), (\pm 2, 0)\}.$$

Por consiguiente, la biyección entre C_2 y E_2 que hemos descrito al tratar el problema de los números congruentes en la Sección 3.1 demuestra que el número 2 no es congruente.

EJEMPLO 4.4. Sean E_{13} y E_{157} las curvas $y^2 = x^3 - n^2x$, con $n = 13$ y 157 respectivamente. Estas curva tienen multiplicación compleja (por $\mathbb{Z}[i]$) y los valores de $L(E_{13}, 1)$ y $L(E_{157}, 1)$ son cero en cualquier precision que usemos (en Magma o Sage, por ejemplo). Los valores de las primeras derivadas son

$$L'(E_{13}, 1) = 4{,}24156537851\ldots \quad \text{y} \quad L'(E_{157}, 1) = 11{,}42594450\ldots$$

Por tanto, BSD predice que $E_{13}(\mathbb{Q})$ y $E_{157}(\mathbb{Q})$ son infinitos, pero el teorema de Coates-Wiles no es suficiente para demostrarlo. Más tarde, en 1986, Gross y Zagier demostraron que si E es *modular* (véase la Sección 6) y $L(E, s)$ tiene un cero de orden 1 en $s = 1$, entonces $E(\mathbb{Q})$ es infinito. Volveremos a este problema en el ejemplo 6.1.

La conjetura BSD tiene otras consecuencias respecto al problema de los números congruentes. Por ejemplo, en 1975 Stephens demostró que BSD implica que todos los números naturales $n \equiv 5$, 6 ó 7 mód 8 son números congruentes. Por ejemplo, $n = 157 \equiv 5$ mód 8 tiene que ser un número congruente y Zagier encontró un triángulo (a, b, c) de área 157. La hipotenusa del triángulo rectángulo más simple de área 157 es:

$$c = \frac{224403517704336969924557513090667486316094847204 1}{8912332268928859588025535178967163570016480830}.$$

Por otra parte, Tunnell demostró en 1983 que si n es un número congruente impar y libre de cuadrados, entonces tenemos una igualdad de cantidades

$$\begin{aligned} &\#\{(x, y, z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2\} \\ &= \frac{1}{2}\left(\#\left\{(x, y, z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2\right\}\right) \end{aligned}$$

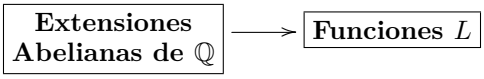
Además, si BSD es cierto, entonces el enunciado recíproco también es cierto: si estas cantidades son iguales, entonces n es un número congruente. El lector puede usar el resultado de Tunnell para demostrar que 13 es congruente (si se cree la conjetura de BSD).

5. Mazur-Wiles

Mazur, B., Wiles, A., Class fields of abelian extensions of **Q**.
Invent. Math. **76** (1984), no. 2, 179-330.

Wiles, A., The Iwasawa conjecture for totally real fields.
Ann. of Math. (2) **131** (1990), no. 3, 493-540.

En estos artículos, [24] y [42], Mazur y Wiles demostraron la conjetura conocida como la «Conjetura Central» de la teoría de Iwasawa (sobre $\mathbb{Q}$), y Wiles demostró la misma conjetura para cuerpos totalmente reales. Esta conjetura proporciona otra relación entre la teoría algebraica de números y funciones L.



La Conjetura Central dice que cierta función L se puede usar para describir la estructura de Galois de ciertas extensiones abelianas de $\mathbb{Q}$ (véase la Sección 11 de [22]). Muy *grosso modo*, la conjetura dice que la estructura del grupo de Galois de cierta extensión infinita de $\mathbb{Q}$ es $\mathbb{Z}_p[[X]]/(L_p(X))$, donde la serie $L_p(X)$ es una función L (p-ádica) cuyos valores críticos vienen dados por expresiones en términos de números de Bernoulli.

El enunciado de la conjetura es muy técnico y no vamos a intentar escribirlo aquí de forma precisa, pues de poco serviría al público en general. Por otra parte, hay muy buenas referencias (en inglés) sobre la teoría de Iwasawa y la Conjetura Central. El libro de Washington, [41], es una de las referencias más completas y más recomendables para aquel que esté comenzando en este tema, al igual que libro de Coates y Sujatha, [3]. El autor también recomienda encarecidamente el artículo [16] de Greenberg, que explica varias de las nuevas tendencias en la teoría de Iwasawa (por ejemplo, las aplicaciones al estudio de rangos de curvas elípticas). El autor escribió para La Gaceta una introducción a la teoría de Iwasawa desde el punto de vista del último teorema de Fermat ([22]).

6. Wiles y Taylor-Wiles

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

Taylor, R.; Wiles, A., Ring-theoretic properties of certain Hecke algebras.
Ann. of Math. (2) **141** (1995), no. 3, 553-572.

En 1993, Wiles anunció una demostración de la *conjetura de la modularidad* en el caso de curvas elípticas semiestables (término definido en el ejemplo 3.8) durante unas charlas en el Instituto Isaac Newton de Ciencias Matemáticas, pero durante el proceso de revisión de su artículo se encontró un error en la demostración. Con la ayuda de uno de sus antiguos doctorandos, Richard Taylor, Wiles consiguió corregir el error, y la demostración se publicó en [43] y [38]. La prueba de la conjetura de

la modularidad para todas las curvas elípticas, debida a Breuil, Conrad, Diamond y Taylor ([2]), tuvo que esperar hasta el año 2001.

Formas Modulares ⇜⇝ **Curvas Elípticas**

La conjetura de la modularidad, también conocida como la conjetura de Shimura-Taniyama-Weil, o conjetura de Shimura-Taniyama (o Taniyama-Shimura), tiene una accidentada historia, que Lang recogió en su artículo [19], donde la llama «una de las más importantes del siglo» (veinte, se entiende). Taniyama presentó una versión preliminar de la conjetura en 1955, y Shimura y Taniyama presentaron un enunciado más refinado en 1957. En 1967, Weil demostró que la conjetura (que no atribuyó a Shimura y Taniyama) sería cierta si las funciones L de las curvas elípticas satisfacieran identidades que ya habían sido conjeturadas con anterioridad (por Hasse, por ejemplo, antes de 1954).

La conjetura de la modularidad se puede enunciar de varias maneras. Esencialmente dice que las curvas elípticas sobre $\mathbb{Q}$ son *modulares*, es decir, cada curva elíptica está asociada a una forma modular. Veamos varias formulaciones concretas de la conjetura de la modularidad. Sea E una curva elíptica definida sobre $\mathbb{Q}$. Decimos que E es modular si se cumplenlas siguientes propiedades (todas ellas equivalentes).

(A) Existe una forma modular $f(z) = \sum_{n\geq 1} a_n(f)q^n$ tal que $a_p(f) = a_p(E) = p + 1 - \#E(\mathbb{F}_p)$, para todo primo p.

(B) Existe una forma modular cuspidal f que es autovector del operador de Hecke T_p, y el coeficiente $a_p = p+1-\#E(\mathbb{F}_p)$ es el autovalor de f, para todo número primo p.

(C) Existe una forma modular f tal que $L(f, s) = L(E, s)$, es decir, las funciones L asociadas a f y a E coinciden.

(D) Existe una forma modular f tal que las representaciones de Galois ρ_{f,p^n} y ρ_{E,p^n} coinciden, para todo primo p y todo $n \geq 1$.

(E) Hay un número $N \geq 1$ tal que existe una función holomorfa y sobreyectiva de superficies de Riemann compactas $X_0(N) \to E$.

(F) Hay un número $N \geq 1$ tal que existe un homomorfismo holomorfo de variedades abelianas $J_0(N) \to E$, donde $J_0(N)$ es la variedad jacobiana de $X_0(N)$.

(G) Hay un número $N \geq 1$, una forma modular cuspidal f de peso 2 y nivel N, y un homomorfismo holomorfo de variedades abelianas $A_f \to E$, donde A_f es la variedad mencionada en el ejemplo 3.10.

EJEMPLO 6.1. Sea E_{13} la curva $y^2 = x^3 - 169x$. Como hemos explicado en el ejemplo 3.8, esta curva tiene reducción aditiva en $p = 2, 13$ así que no es semiestable (y el teorema de Taylor-Wiles no se puede usar en este caso). Aun así, en el ejemplo 3.11 hemos mencionado que E_{13} es igual a la variedad abeliana A_f que corresponde a la forma modular $f(z) = q + 2q^5 - 3q^9 + 2q^{17} - q^{25} + \cdots$, y $A_f \cong E_{13}$ es por tanto una curva modular (como *todas* las curvas elípticas sobre $\mathbb{Q}$, por el teorema de la modularidad). También hemos visto que $L(E_{13}, s) = L(f, s)$ en el ejemplo 3.8.

Hemos mencionado en el ejemplo 4.4 que Gross y Zagier demostraron que si E es *modular* y $L(E,s)$ tiene un cero de orden 1 en $s=1$, entonces $E(\mathbb{Q})$ es infinito (que es un caso particular de la conjetura de Birch y Swinnerton-Dyer). Como E_{13} es modular, $L(E_{13},1)=0$ y $L'(E_{13},1)\neq 0$, podemos concluir que $E_{13}(\mathbb{Q})$ es un conjunto infinito y por tanto el número 13 es congruente.

Una búsqueda de puntos en E_{13} (a lo bruto, o usando el método de descenso) desvela que el punto $(-36/25, 1938/125)$ pertenece a E_{13} y, usando la biyección $f: E_n \to C_n$ del ejemplo 3.1, podemos construir el triángulo rectángulo de lados $\left(\frac{323}{30}, \frac{780}{323}, \frac{106921}{9690}\right)$ que tiene área 13.

Ejemplo 6.2. La demostración de la conjetura de la modularidad (en el caso semiestable) fue el último paso para demostrar el último teorema de Fermat, cuyo enunciado dice que la ecuación $x^n + y^n = z^n$ no tiene soluciones en enteros $x, y, z \in \mathbb{Z}$, con $xyz \neq 0$, cuando $n \geq 3$.

Figura 9: Pierre de Fermat (1601-1665).

La estrategia que culminó en la primera demostración (correcta) del último teorema de Fermat fue propuesta por Hellegouarch, Frey ([15]) y Serre ([31]). Sea $p \geq 11$ un primo y supongamos que a, b, c son enteros primos entre sí tales que $a^p + b^p = c^p$ y $abc \neq 0$. En 1972, Hellegouarch sugirió estudiar la curva elíptica

$$E: y^2 = x(x - a^p)(x + b^p).$$

En 1984, Frey descubrió que esta curva elíptica sería semiestable y, además, propuso que la curva E no podría ser modular si existiera. El problema con la modularidad de E lo hizo preciso Serre y lo redujo a una conjetura, llamada la *conjetura épsilon*. Ribet ([27]) demostró la conjetura épsilon en 1986, con lo cual quedaba demostrado que si E existiera, sería una curva elíptica definida sobre $\mathbb{Q}$ y semiestable, pero no modular.

Finalmente, en 1995, Wiles ([43]) y Taylor y Wiles ([38]) demostraron la conjetura de la modularidad para curvas elípticas semiestables. Así que $E: y^2 = x(x-a^p)(x+$

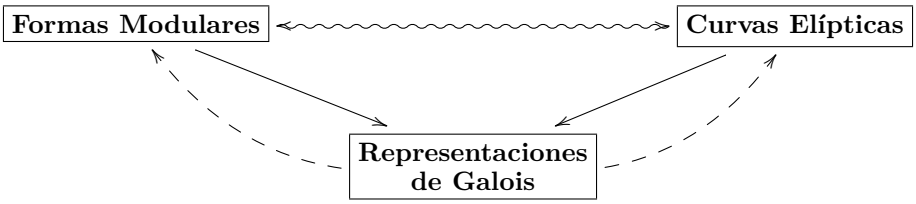
b^p) sería modular si existiera, en contradicción con el teorema de Ribet, y por tanto concluyeron la prueba del último teorema de Fermat.

7. SKINNER-WILES

Skinner, C. M.; Wiles, A. J. Ordinary representations and modular forms. *Proc. Nat. Acad. Sci. U.S.A.* **94** (1997), no. 20, 10520-10527.

Skinner, C. M.; Wiles, A. J.
Residually reducible representations and modular forms.
Inst. Hautes Études Sci. Publ. Math. no. **89** (1999), 5-126 (2000).

El teorema de la modularidad crea un puente entre curvas elípticas y formas modulares. Por otra parte, en la Sección 3.4 hemos visto que podemos definir representaciones de Galois a partir de formas modulares y curvas elípticas, y una pregunta natural es si se pueden construir objetos geométricos a partir de representaciones de Galois. En otras palabras, ¿son todas las representaciones de Galois «modulares» o «geométricas»?



La conjetura de Fontaine-Mazur ([14]) predice que toda representación de Galois que cumple unas propiedades básicas proviene de la geometría o del mundo automorfo (que en muchos casos es lo mismo, por modularidad). Con un poco más de detalle, la conjetura dice que si $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(n, \mathbb{Q}_p)$ es una representación de Galois que es *potencialmente semiestable* (no vamos a definir este término técnico) y se ramifica solo en un número finito de primos, entonces ρ se puede reconstruir por la acción de Galois en la cohomología de alguna variedad algebraica, o a través de las representaciones asociadas a las variedades abelianas que provienen de formas modulares.

El lector puede encontrar un enunciado más detallado en [14], o en el artículo [39], que es una versión ampliada de la conferencia de Taylor en el ICM del 2002.

EJEMPLO 7.1. Sea $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Q}_p)$ una representación de Galois que es potencialmente semiestable, y cuyo determinante es impar (esta última propiedad quiere decir que el determinante de la imagen de cualquier conjugación compleja debe ser -1). Entonces, la conjetura de Fontaine-Mazur implica que ρ es modular, es decir, proviene de una forma modular.

Ahora, sea $\rho = \rho_{E,p^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(T_p(E)) \cong \mathrm{GL}(2, \mathbb{Z}_p)$ la representación p-ádica asociada a una curva E sobre $\mathbb{Q}$, definida en ejemplo 3.10. Un teorema de Tsuji (el teorema de comparación) demuestra que las representaciones que provienen

Figura 10: Jean Marc Fontaine y Barry Mazur.

de la geometría son potencialmente semiestables. Por otra parte, es fácil ver que la imagen de una conjugación compleja a traves de ρ_{E,p^∞} tiene determinante -1 (por ejemplo, usando que $\det(\rho_{E,p^\infty}) = \chi_{p^\infty}$ es el carácter p-ádico ciclotómico).

En los artículos [34] y [35], Skinner y Wiles demuestran nuevos casos de la conjetura de Fontaine-Mazur. En Taylor-Wiles, para probar la conjetura de la modularidad (semiestable), habían demostrado la conjetura de Fontaine-Mazur en el caso de una representación 2-dimensional $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Q}_p)$ tal que la reducción ρ módulo p es absolutamente irreducible. En Skinner-Wiles, consiguen demostrar Fontaine-Mazur cuando la reducción ρ mód p es reducible, generando muchas nuevas ideas y técnicas en el proceso. Estas técnicas han sido depuradas por Kisin ([17]) para demostrar, en 2009, la conjetura de Fontaine-Mazur en el caso 2-dimensional (salvo en algunos casos excepcionales).

Referencias

[1] A. D. Aczel, *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem*, Basic Books, 2007, o su traducción *Último Teorema de Fermat: El Secreto de un Antiguo Problema Matemático*, Fondo de Cultura Economica, Sección de Obras de Ciencia y Tecnología, 2004.

[2] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over Q: Wild 3-adic exercises, *Journal of the American Mathematical Society* 14 (2001), 843-939.

[3] J. Coates, R. Sujatha, *Cyclotomic Fields and Zeta Values*, Springer, 2009.

[4] J. Coates, S. T. Yau (editores), *Elliptic Curves, Modular Forms, and Fermat's Last Theorem*, Proceedings of a conference held in the Institute of Mathematics of the Chinese University of Hong Kong, 2nd Edition, International Press, 1997.

[5] J. Coates, J., A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* 39 (1977), no. 3, 223-251.

[6] H. COHN, A. KUMAR, S. D. MILLER, D. RADCHENKO, M. VIAZOVSKA, The sphere packing problem in dimension 24, http://arxiv.org/abs/1603.06518

[7] B. CONRAD, K. RUBIN (Editores), *Arithmetic Algebraic Geometry*, AMS, IAS/Park City Mathematics Series Volume 9, 2001.

[8] K. E. CONRAD, *The Congruent Number Problem*, disponible en su página: http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/congnumber.pdf

[9] G. CORNELL, J. H. SILVERMAN, G. STEVENS (editores), *Modular forms and Fermat's last theorem* (Boston, MA, 1995), Springer, New York, 1997.

[10] D. A. COX, Introduction to Fermat's Last Theorem, *Amer. Math. Monthly* 101 (1994), 3-14.

[11] F. DIAMOND, J. SHURMAN, *A First Course in Modular Forms*, Graduate Texts in Mathematics 228, Springer-Verlag, 2nd Edition, New York, 2005.

[12] L. E. DICKSON, *History of the Theory of Numbers, Volume II: Diophantine Analysis*, Dover Publications, 2005.

[13] H. M. EDWARDS, *Fermat's last theorem: A genetic introduction to algebraic number theory*, GTM 50, Springer, 1977.

[14] J. M. FONTAINE, B. MAZUR, *Geometric Galois representations, elliptic curves, modular forms, and Fermat's last theorem* (Hong Kong, 1993), Internat. Press, Cambridge, MA, 41-78, 1995.

[15] G. FREY, Links between solutions of $A - B = C$ and elliptic curves. *Number theory (Ulm, 1987)*, 31-62, Lecture Notes in Math., 1380, Springer, New York, 1989.

[16] R. GREENBERG, *Iwasawa Theory - Past and Present*, disponible en su página: http://www.math.washington.edu/~greenber/research.html

[17] M. KISIN, The Fontaine-Mazur conjecture for GL2. *J. Amer. Math. Soc.* 22 (2009), no. 3, 641-690.

[18] NEAL I. KOBLITZ, *Introduction to Elliptic Curves and Modular Forms*, Second Edition, Springer-Verlag, New York, 1993.

[19] S. LANG, Some history of the Shimura-Taniyama conjecture, *Notices of the AMS*, Vol. 41, Number 11, November 1995, 1301-1307.

[20] Á. LOZANO-ROBLEDO, Buscando puntos racionales en curvas elípticas: Métodos explícitos, *Gac. R. Soc. Mat. Esp.* 8 (2005), no. 2, 471-488.

[21] Á. LOZANO-ROBLEDO, Bernoulli numbers, Hurwitz numbers, p-adic L-functions and Kummer's criterion, *RACSAM*, Vol 101 (1), 2007, 1-32.

[22] Á. LOZANO-ROBLEDO, Desde Fermat, Lamé y Kummer hasta Iwasawa: Una introducción a la teoría de Iwasawa, *Gac. R. Soc. Mat. Esp.* 15 (2012), no. 2, 251-276.

[23] Á. LOZANO-ROBLEDO, *Elliptic curves, modular forms, and their L-functions*, Student Mathematical Library, 58, IAS/Park City Mathematical Subseries. American Mathematical Society, Providence, RI; Institute for Advanced Study (IAS), Princeton, NJ, 2011.

[24] B. MAZUR, A. WILES, Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.* 76 (1984), no. 2, 179-330.

[25] J. S. Milne, *Elliptic curves*, BookSurge Publishers, Charleston, SC, 2006.

[26] C. Popescu, K. Rubin, A. Silverberg (editores), *Arithmetic of L-Functions*, AMS, IAS/Park City Mathematics Series Volume 18, 2011.

[27] K. A. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Invent. Math.* 100 (1990), no. 2, 431-476.

[28] K. A. Ribet, Galois representations and modular forms, *Bull. Amer. Math. Soc. (N.S.)*, 32 (1995), no. 4, 375-402.

[29] T. Saito, *Fermat's last theorem. The proof*, Translated from the 2009 Japanese original by Masato Kuwata. Translations of Mathematical Monographs, 245. Iwanami Series in Modern Mathematics. American Mathematical Society, Providence, RI, 2014.

[30] S. Singh, *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem*, 1st Anchor Books, 1998, o su traducción *El Enigma de Fermat*, Editorial Ariel, 2015.

[31] J. P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.* 54 (1987), no. 1, 179-230.

[32] J. H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

[33] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 2nd Edition, New York, 2009.

[34] C. M. Skinner, A. Wiles, Ordinary representations and modular forms. *Proc. Nat. Acad. Sci. U.S.A.* 94 (1997), no. 20, 10520-10527.

[35] C. M. Skinner, A. Wiles, Residually reducible representations and modular forms. *Inst. Hautes Études Sci. Publ. Math.* No. 89 (1999), 5-126 (2000).

[36] W. Stein, *Modular Forms, a computational approach*, American Mathematical Society, 2007.

[37] W. Stein, *Elementary Number Theory: Primes, Congruences, and Secrets: A Computational Approach*, Undergraduate Texts in Mathematics, Springer, New York, 2008.

[38] R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.* (2) 141 (1995), no. 3, 553-572.

[39] R. Taylor, Galois Representations, *Annales de la faculté des sciences de Toulouse* (2004) Tome XIII, no. 1, 73-119. .

[40] M. Viazovska, The sphere packing problem in dimension 8, `https://arxiv.org/pdf/1603.04246`

[41] L. C. Washington, *Introduction to cyclotomic fields*, Second Edition, GTM 83, Springer, 1997.

[42] A. Wiles, The Iwasawa conjecture for totally real fields. *Ann. of Math.* (2) 131 (1990), no. 3, 493-540.

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

[44] A. Wiles The Birch and Swinnerton-Dyer conjecture, *The Millennium prize problems*. American Mathematical Society, 31-44.

ÁLVARO LOZANO-ROBLEDO, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CONNECTICUT, STORRS, CT 06269, USA
Correo electrónico: alvaro.lozano-robledo@uconn.edu
Página web: http://alozano.clas.uconn.edu