UN VISTAZO AL TRABAJO DE ANDREW WILES

NUNO FREITAS

El revolucionario trabajo de Andrew Wiles sobre la modularidad de las curvas elípticas semiestables sobre $\mathbb{Q}$ ha sido uno de los grandes logros matemáticos de finales del siglo XX. Las ideas de Wiles causaron un tremendo impacto en Teoría de Números, ya que han tenido fuertes consecuencias en algunas de sus principales áreas de investigación, como el Programa de Langlands o las Ecuaciones Diofánticas. Dada su enorme contribución en el campo de las matemáticas, incluyendo la demostración completa del Último Teorema de Fermat, Andrew Wiles ha sido recientemente galardonado con el Premio Abel 2016.

La conjetura de Shimura–Tanyama–Weil. La Conjetura S–T–W relaciona curvas elípticas y formas modulares, dos objetos que viven en mundos diferentes sin, a priori, ninguna relación aparente.

Una *curva elíptica sobre* $\mathbb{Q}$ es una ecuación cúbica

$$E:\ y^2 = x^3 + ax + b, \quad a, b, \in \mathbb{Q}, \qquad \Delta_E = -2^4(4a^3 + 27b^2) \neq 0. \tag{1}$$

Desde hace mucho tiempo ha habido un fuerte interés por encontrar soluciones racionales de estas ecuaciones cúbicas, i.e. pares (x, y) satisfaciendo (1) y tales que x e y pertenecen a $\mathbb{Q}$. De hecho, el estudio de las curvas elípticas data de la Antigua Grecia, donde *el proceso de cuerdas y tangentes* para la construcción de nuevas soluciones racionales a partir de las conocidas ya era utilizado. Hoy en día este método puede ser resumido concisamente utilizando uno de los resultados más fundamentales en la teoría de curvas elípticas: el Teorema de Mordell-Weil. Este resultado afirma que el conjunto formado por *todas* las soluciones racionales $E(\mathbb{Q})$ de (1), junto al punto del infinito, tiene estructura algebraica de grupo abeliano *finitamente* generado. En otras palabras, existe un conjunto finito de soluciones racionales de (1) a partir del cual se pueden obtener todas las demás soluciones racionales por el método de cuerdas y tangentes. La existencia de esta estructura de grupo convierte a las curvas elípticas en una clase especial de curvas.

Un enfoque que se ha mostrado especialmente útil en el estudio de ecuaciones Diofánticas como (1) es el uso de congruencias. Dada la ecuación (1), tras un cambio de coordenadas lineal, podemos asumir que los coeficientes de E pertenecen a $\mathbb{Z}$ y que Δ_E es minimal. Para $p \nmid \Delta_E$ primo, el conjunto de soluciones de (1) modulo p son todos los pares $(x, y) \in \mathbb{F}_p^2$ tales que $y^2 \equiv x^3 + ax + b \bmod p$, donde $\mathbb{F}_p$ es el cuerpo finito de p elementos. Sea N_p el número de todas estas soluciones, considerando también el punto del infinito. Se define $a_p(E) = p + 1 - N_p$, el término de error entre el número de soluciones módulo p y el número de puntos en el espacio proyectivo $\mathbb{P}^1(\mathbb{F}_p)$. Un resultado clave llamado Teorema de Hasse para curvas elípticas nos dice que $-2\sqrt{p} \leq a_p \leq 2\sqrt{p}$. La definición de a_p se puede extender también a los primos $p \mid \Delta_E$, en cuyo caso $a_p \in \{-1, 0, 1\}$. En el proceso, obtenemos otra cantidad N_E llamada el *conductor* de E: un número natural que da una medida de la complejidad aritmética de E.

Una *forma modular de peso* 2 *para* $\Gamma_0(N)$ ($N \in \mathbb{Z}_{\geq 1}$) es una función analítica f con dominio en el semiplano complejo superior, que satisface ciertas condiciones de

crecimiento y tal que

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$$

para cada matriz $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ tal que $N \mid c$. La invariancia de f por translaciones implica la existencia de la siguiente expansión de Fourier

$$f(z) = \sum_{n=0}^{\infty} a_n(f) q^n, \qquad q = e^{2\pi i z}.$$

Se llaman *formas cuspidales* aquellas que satisfacen $a_0(f) = 0$. La *Conjetura de Shimura–Tanyama–Weil* afirma que para cada curva elíptica $E/\mathbb{Q}$ de conductor N_E existe una forma cuspidal f de peso 2 para $\Gamma_0(N_E)$, normalizada en el sentido que $a_1(f) = 1$, y tal que para todo primo p los coeficientes de Fourier satisfacen $a_p(f) = a_p(E)$. En este caso se dice que la curva E es *modular*.

En su articulo seminal [2] y en [1] (conjuntamente con R. Taylor), Andrew Wiles dio una demostración de la Conjetura S-T-W para el caso de curvas elípticas *semiestables*, i.e. curvas elípticas de conductor N_E libre de cuadrados.

Ecuaciones Diofánticas. El Último Teorema de Fermat, formulado inicialmente por Pierre de Fermat en el siglo XVII, afirma que la ecuación $x^n + y^n = z^n$, con $n > 2$, no tiene solución en enteros tales que $xyz \neq 0$. Fermat demostró el caso particular $n = 4$, Leonhard Euler dio una prueba para $n = 3$, y Sophie Germain fue la primera en demostrar un resultado más general, probando el teorema cuando el exponente n y $2n + 1$ son primos suponiendo que $n \nmid xyz$. Hubo que esperar 350 años tras la formulación original de Fermat para conseguir una demostración para todo $n > 2$, uno de los principales resultados del trabajo de Wiles.

La conexión entre el Último Teorema de Fermat y la modularidad es ciertamente sorprendente, y es fruto del trabajo de Frey, Mazur, Serre y Ribet. A cada presunta solución (a, b, c) de la ecuación de Fermat, con $abc \neq 0$, se le asocia una curva elíptica, llamada *curva de Frey o Frey-Hellegouarch*,

$$E_{a,b,c} \; : \; Y^2 = X(X - a^p)(X + b^p)$$

que, salvo múltiplos y permutaciones de la solución, se puede asumir semiestable. Suponiendo cierta la Conjetura S-T-W, del trabajo de Mazur y Ribet se concluye que la representación módulo p de $E_{a,b,c}$ debe ser modular de nivel 2, cosa imposible. En otras palabras, si la solución (a, b, c) existe, entonces existe una curva elíptica semiestable que no es modular, pero gracias al trabajo de Wiles hoy en día se sabe que tales curvas no existen.

La demostración del Último Teorema de Fermat ha sido el inicio de una nueva era en el mundo de las ecuaciones Diofánticas. La estrategia revolucionaria de su demostración, conocida como *el método modular*, ha tenido muchas extensiones, y en consecuencia se han podido solucionar muchas otras ecuaciones que previamente se consideraban imposibles. El nuevo Santo Grial es la Ecuación de Fermat Generalizada

$$x^p + y^q = z^r, \qquad 1/p + 1/q + 1/r < 1, \qquad \gcd(x, y, z) = 1, \qquad xyz \neq 0.$$

Se conjectura que esta ecuación sólo tiene una cantidad finita de soluciones, y prácticamente todo lo que se sabe hoy en día apuntando en esta dirección ha sido establecido usando extensiones del método modular. También es digno de mención que el método modular no solo permite atacar ecuaciones ternarias como las anteriores, sino que también tiene aplicaciones en problemas más clásicos y sin relación aparente, como es el encontrar potencias perfectas en secuencias de Fibonacci.

El Programa de Langlands. Un objeto de estudio fundamental en la teoría de números moderna es el grupo absoluto de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Este es el grupo de automorfismos del cuerpo $\overline{\mathbb{Q}}$, definido como el conjunto de todas las raíces complejas de polinomios (mónicos) con coeficientes racionales. Una *representación de Galois* es una representación finito-dimensional $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(F)$, para cualquier cuerpo F. Más en general, podemos reemplazar $\mathbb{Q}$ por cualquier cuerpo de números.

Existe una formulación equivalente de la Conjetura S-T-W en términos de representaciones de Galois asociadas a curvas elípticas y formas modulares. Desde este punto de vista, el trabajo de Wiles se puede interpretar como una conexión entre formas automorfas (objetos de teoría de representación de grupos adélicos) y representaciones de Galois, perteneciendo así a una gran red de conjeturas llamada *el Programa de Langlands*.

Las ideas de Wiles introdujeron un nuevo y notable método para atacar esta línea de conjeturas. En los últimos 21 años, se han solucionado muchas otras conjeturas importantes, cuyas pruebas están fuertemente basadas en refinamientos y generalizaciones de las ideas de Wiles:

- la totalidad de la Conjetura de S-T-W por Breuil, Conrad, Diamond and Taylor;
- la Conjetura de Artin (bajo algunas condiciones técnicas) para representaciones icosaédricas $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ por Taylor, Buzzard, Dickinson y Shepherd–Barron;
- generalizaciones de teoremas de levantamiento de modularidad a cuerpos de números totalmente reales, por Skinner–Wiles y Fujiwara;
- generalizaciones de teoremas de levantamiento de modularidad a dimensiones superiores, por Clozel, Harris, Shepherd–Barron, Taylor y Thorne; En particular, dando lugar a la prueba de la conjetura de Sato-Tate;
- la Conjetura de Fontaine-Mazur (bajo condiciones suaves) para el caso GL_2 por Kisin;
- La Conjetura de Serre por Khare–Wintenberger, Kisin y Dieulefait. En particular, dando lugar a la prueba de la conjetura completa de Artin en el caso impar, por Khare;
- La Conjetura de Sato-Tate para formas modulares de Hilbert, por Barnet-Lamb, Gee y Geraghty;
- la Conjetura S-T-W sobre cuerpos cuadráticos reales por Freitas–Le Hung–Siksek.

References

[1] R. Taylor and A. Wiles *Ring-theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.

[2] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.