

# Introducción a la modularidad de curvas elípticas: Un enfoque teórico-computacional

(Propuesta de Curso para la XXIII Escuela Venezolana de Matemáticas)

Enrique González Jiménez  
Universidad Autónoma de Madrid  
Departamento de Matemáticas  
28049 Madrid, España  
email : enrique.gonzalez.jimenez@uam.es

Amílcar J. Pérez A.  
Universidad Simón Bolívar  
Departamento de Matemáticas Puras y Aplicadas  
8900 Baruta, Venezuela  
email : ajperez@usb.ve

## 1. INTRODUCCIÓN HISTÓRICO-MATEMÁTICA

Uno de los resultados más notables de las matemáticas de los últimos siglos ha sido la consecución de una prueba del Último Teorema de Fermat (UTF): la ecuación  $x^n + y^n = z^n$  con  $n \geq 3$  entero, no tiene soluciones enteras tales que  $xyz \neq 0$ . Alrededor de 1630 el mismo Fermat probó su conjetura para  $n = 4$ . Sin embargo con respecto al caso general Fermat sólo afirmó tener una prueba maravillosa que no cabía en aquel exiguo margen. Inmediatamente se fue claro que bastaba probar el UTF para  $n \geq 3$  primo.

En 1753, más de cien años después de la prueba de Fermat, Leonhard Euler publicó una prueba para  $n = 3$  (una de las primeras instancias donde aparecen números algebraicos). Cerca de tres cuartos de siglo más tarde, en 1825 y casi simultáneamente, Gustav P. L. Dirichlet y Adrien M. Legendre probaron el UTF para  $n = 5$ . El siguiente logro puntual lo obtuvo Gabriel Lamé en 1839 para  $n = 7$ , su prueba aún más intrincada que las anteriores, daba mayores indicios de la necesidad de otra forma de atacar el problema general.

Aunque el primer resultado general lo halló Sophie Germain alrededor de 1820 al probar la validez de UTF para  $n$  y  $2n + 1$  primos y  $xyz$  no divisible por  $n$ , fue el trabajo de Ernst Kummer en los años cercanos a 1847, el que mostraría un enfoque muy próximo al moderno. Kummer definió el grupo de clases del cuerpo ciclotómico asociado a las raíces  $n$ -ésimas de la unidad, demostró que su orden  $h_n$  es finito, y probó el UTF para  $n$  un primo regular, i.e.,  $n$  un primo que no divide a  $h_n$ . Sin embargo aún hoy no se sabe si hay infinitos primos regulares, aunque paradójicamente se ha probado la infinitud de los primos no regulares.

No obstante, Kummer caracterizó los primos regulares hallando una fórmula, enraizada en la fórmula analítica de Dirichlet del número de clases, que vincula un factor de  $h_n$  (conectado con el número de clases del subcuerpo real del cuerpo ciclotómico mencionado) con valores especiales de ciertas  $L$ -series  $L(\chi, s)$  (asociadas a determinados caracteres de Dirichlet  $\chi$ ) en términos de números de Bernoulli generalizados  $B_{i,\chi}$ , relacionados con los números de Bernoulli  $B_i$  vía congruencias módulo  $n$ . Esta conexión entre el número de clases y propiedades de congruencias de valores especiales de funciones  $L$  aparece también en la prueba final de Wiles y Taylor–Wiles del UTF para  $n$  primo.

El siguiente avance teórico significativo lo obtuvo Gerd Faltings en 1983 al probar la siguiente conjetura de Mordell: una ecuación en dos variables con coeficientes racionales, correspondiente a una curva de género  $g \geq 2$  tiene a lo más un número finito de soluciones racionales. Así, la ecuación de Fermat reescrita en forma afín  $X^n + Y^n = 1$  con  $n \geq 4$  y por tanto de género  $g \geq 3$ , tiene a lo más un número finito de soluciones. Sin embargo la idea sobre la cual descansaría la prueba final fue observada por Gerhard Frey en 1985, formulada en términos precisos como la conjetura  $\varepsilon$  por Jean P. Serre en 1986, y probada ese mismo año por Kent Ribet. Esencialmente el teorema de Frey–Serre–Ribet reducía el problema de probar el UTF a probar la conjetura de Shimura–Taniyama–Weil sobre la modularidad de una curva elíptica definida sobre los racionales, en el caso especial de las curvas elípticas semiestables, i.e., de conductor libre de cuadrados.

Suponiendo que existe una solución no trivial,  $a, b, c$  de la ecuación de Fermat  $a^n + b^n = c^n$ , con  $n \geq 11$  primo, Frey asoció a ésta la curva elíptica semiestable:

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

Si  $E[n]$  es el subgrupo de puntos de  $E$  de orden  $n$ , sobre la clausura algebraica de los racionales  $\bar{\mathbb{Q}}$  y  $G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  es el grupo absoluto de Galois, entonces es posible asociar a  $E$ , vía la acción de  $G_{\mathbb{Q}}$

sobre  $E[n]$ , una representación:

$$\bar{\rho}_n : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_n)$$

siendo  $\mathbb{F}_n$  el cuerpo finito de  $n$  elementos. En este contexto la conjetura de Serre predice que las representaciones  $\bar{\rho}_n$  provienen de formas modulares de peso 2 y nivel 2 (funciones complejas definidas sobre el semiplano complejo  $\{z \in \mathbb{C} : \text{Im}(z) > 0\}$ , de período 1 y con determinadas propiedades de transformación). Ribet probó esta conjetura, ¡pero tales formas no existen!

Por otro lado, la teoría de Eichler–Shimura asocia a una forma modular propia de Hecke  $f(z)$  de peso 2 y nivel  $N$ , con serie de Fourier racional:

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \quad a_n \in \mathbb{Q} \quad \text{con } q = \exp(2\pi iz)$$

una curva elíptica con coeficientes racionales, de conductor  $N$  y con serie de Dirichlet:

$$L(E, s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s} \quad \text{¡siendo } c_n = a_n!$$

donde los  $c_p$  con  $p$  primo, en un sentido preciso, “cuentan” el número de soluciones de la curva elíptica módulo  $p$ , con  $p$  primo.

La conjetura de Shimura–Taniyama–Weil, ahora teorema, afirma que toda curva elíptica definida sobre los racionales, proviene de una forma modular propia de Hecke en el sentido anterior. Ésta es sólo una de las versiones equivalentes de la modularidad de una curva elíptica definida sobre los racionales. También es posible definir la modularidad de las representaciones de Galois  $\rho_{E,p}$  asociadas a  $E$ . Y un hecho de capital importancia es la siguiente equivalencia:

1.  $E$  definida sobre  $\mathbb{Q}$  es modular
2.  $\rho_{E,p}$  es modular para algún primo  $p$

En 1994 Andrew Wiles probó que  $\rho_{E,3}$  es modular para una curva elíptica semiestable  $E$  definida sobre  $\mathbb{Q}$ , usando entre otros, resultados fundamentales de Langlands–Tunnell y uno complementario de Taylor–Wiles. De este modo Wiles, en virtud de la equivalencia anterior y la conjetura  $\epsilon$  de Serre, dedujo la validez de UTF.

Siguiendo esta línea, en 1999 Breuil, Conrad, Diamond y Taylor completaron la prueba de la conjetura de Shimura–Taniyama en el caso no semiestable. Por otra parte, el trabajo de Wiles sobre la modularidad de una curva elíptica sobre los racionales permite simplificar el enunciado de uno de los problemas del Milenio: La conjetura de Birch y Swinnerton-Dyer, que da una conexión entre un valor especial de  $L(E, s)$  y el rango del subgrupo libre del grupo de puntos racionales de  $E$ , será enunciada en una versión accesible al final del curso.

Aunque el anterior es el contexto de esta propuesta, no obstante ésta tiene un carácter introductorio, como lo reflejan las listas de objetivos y contenidos dadas abajo.

## 2. ASPECTOS COMPUTACIONALES DE LA PROPUESTA

El desarrollo de la moderna teoría de números y concretamente el estudio de curvas elípticas y de formas modulares ha experimentado un notable avance en las últimas décadas probablemente por el gran avance del desarrollo del álgebra computacional orientada a estas áreas. La conjetura de Birch y Swinnerton-Dyer y la teoría de modularidad de curvas elípticas son algunos de los ejemplos más representativos de este desarrollo. Durante la escuela se hará uso del software **SAGE** que nos permitirá trabajar de forma completamente explícita con objetos abstractos como son las curvas elípticas y las formas modulares. Con esto se pretende introducir al estudiante a un área muy abstracta de las matemáticas haciéndola más accesible y “visible” mediante el uso computacional de estos conceptos.

## 3. PRERREQUISITOS

- Haber cursado cursos básicos de álgebra, variable compleja y geometría diferencial.
- Conveniente pero no estrictamente necesario: cursos introductorios a la teoría de números elemental y geometría algebraica básica.
- En el curso se hará uso de forma exclusiva del software libre **SAGE**. Aunque no es estrictamente necesario, un conocimiento previo de **SAGE** o de algún otro software para cálculo simbólico como Mathematica, Maple o Magma sería de gran ayuda.

#### 4. OBJETIVOS

- Introducir a los estudiantes a la resolución de ecuaciones diofánticas con técnicas de la moderna teoría de números y su conexión con la geometría algebraica.
- Propiciar al estudiante una comprensión suficientemente detallada del conocimiento necesario sobre las curvas elípticas sobre los racionales, reales, complejos y cuerpos finitos.
- Mostrar los resultados sobre formas modulares necesarios para comprender la modularidad de las curvas elípticas sobre los racionales.
- Por último presentar en terminos accesibles para el alumno una versión de la anteriormente, ahora teorema, conjetura de Shimura-Taniyama-Weil, la relación de una parte importante de la prueba de esta conjetura y el Último Teorema de Fermat y exponer una versión débil de la Conjetura de Birch y Swinnerton-Dyer.
- Ilustrar los conceptos y técnicas anteriores empleando para ello el software libre **SAGE**.

#### 5. PROGRAMA DEL CURSO

1. Introducción a las ecuaciones diofánticas.
  - Curvas algebraicas planas.
  - Ecuaciones lineales y cuadráticas. Teoremas de Legendre y Hozel.
  - Ecuaciones de grado superior. Género de una curva. Cúbicas. Teorema de Faltings.
2. Curvas elípticas sobre los racionales.
  - Forma de Weierstrass. Cambios admisibles de variables. Modelo mínimo global.
  - Ley de grupo. Teorema de Poincaré. Teorema de Mordell.
  - Subgrupo de torsión. Teoremas de Lutz-Nagell y de Mazur.
  - Rango. Algunas conjeturas.
  - Puntos de coordenadas enteras. Teorema de Siegel.
3. Curvas elípticas sobre cuerpos finitos.
  - Cota de Hasse.
  - Función zeta.
  - Aplicaciones a la Criptografía y a la factorización de enteros. (Tentativo).
4. Curvas elípticas sobre los complejos.
  - Funciones elípticas. Función  $\wp$  de Weierstrass.
  - Ecuación diferencial para  $\wp$ .
  - Uniformización: Curva elíptica como superficie de Riemann. Género geométrico.
  - Funciones  $\Delta$  y  $j$ .
5. Formas modulares.
  - Formas modulares de nivel 1. Operadores de Hecke. Producto escalar de Petersson.  $q$ -expansión.
  - Grupos de congruencia. Formas modulares de nivel superior. Formas cuspidales.
  - Formas nuevas y su cuerpo de coeficientes.
6. Modularidad.
  - Función zeta de Riemann. Ecuación funcional.
  - Función  $L$  de una curva elíptica definida sobre los racionales.
  - Función  $L$  de una forma modular. Ecuación funcional.
  - Conjetura de Shimura-Taniyama-Weil: Teorema de Wiles et al.
  - Construcción explícita de una forma modular a partir de una curva elíptica definida sobre los racionales.
  - Construcción explícita de una curva elíptica definida sobre los racionales a partir de una forma modular nueva con coeficientes racionales.
  - Conjetura de Birch y Swinnerton-Dyer.

#### 6. RECURSOS REQUERIDOS PARA DICTAR EL CURSO

La exposición será fundamentalmente realizada por medio de videoprojector conectado al computador. Aunque en algunos momentos se hará uso de pizarra.

Debido al enfoque computacional se necesitará de un computador para cada uno o dos alumnos. En cada uno de ellos deberá estar instalado el software libre **SAGE**, con el cual se harán todas las prácticas.

## BIBLIOGRAFÍA BÁSICA

- B. Conrad y K. Rubin (Eds) : *Arithmetic algebraic geometry*. AMS, 2001.
- F. Diamond y J. Shurman, *A first course in modular forms*. GTM 228. Springer-Verlag, 2005.
- A.W. Knap, *Elliptic Curves*. Princeton Uni. Press, 1992.
- J.H. Silverman, *The Arithmetic of Elliptic Curves*. GTM 106, Springer-Verlag, 1986.
- J.H. Silverman y J. Tate, *Rational points on elliptic curves*. UTM. Springer-Verlag, 1992.
- W. A. Stein. *Modular forms, a computational approach*. AMS, 2007. (<http://wstein.org/books/modform>).
- W. Stein et al. *Sage: Open Source Mathematical Software*, 2009, <http://www.sagemath.org>.

## BIBLIOGRAFÍA EVM

- L. Gómez Sánchez. *Invitación al estudio de la aritmética de curvas elípticas*. Año 1993.
- J. Tena Ayuso. *Curvas elípticas en criptografía*. Año 1995.
- F. Rodríguez Villegas. *Introducción a las funciones zeta de Hasse-Weil*. Año 1999.

## BIBLIOGRAFÍA ADICIONAL

- T. M. Apostol, *Modular functions and Dirichlet series in Number Theory*, Springer-Verlag, 1990.
- G. Cornell, J. Silverman y G. Stevens, *Modular forms and Fermat's last theorem*, Springer, 1997.
- H. Darmon, F. Diamond y R. Taylor, *Fermat's last theorem, Elliptic curves, modular forms and Fermat's last theorem*, Hong Kong, **1993**, 2-140, 1995.
- F. Gouvea, *A marvelous proof*, Ame. Math. Monthly, **101**, 203-222, 1994.
- A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), 443-551.