CURSO AVANZADO DE ÁLGEBRA

Máster en Matemáticas y Aplicaciones
2º Cuatrimestre - Curso 2011–12

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

OBJETIVO DEL CURSO

Este curso se enmarca dentro de la especialidad *Iniciación a la investigación* del *Máster en Matemáticas y Aplicaciones* de la *Universidad Autónoma de Madrid*. El objetivo principal de este curso es el estudio de algunas ideas que subyacen en la demostración del Teorema de Modularidad (antigua conjetura de Shimura-Taniyama-Weil) y en particular del Último Teorema de Fermat. Por otro lado, 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 el curso se hará uso del software `SAGE` y/o `Magma` 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 algunos de estos conceptos.
Los objetivos principales de este curso son:
− 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 la Conjetura de Birch y Swinnerton-Dyer.
− Ilustrar los conceptos y técnicas anteriores empleando para ello el software libre `SAGE` y/o `Magma`.

PROGRAMA

1. Introducción a las ecuaciones diofánticas.
   - Curvas algebraicas planas.
   - Ecuaciones de grado 2: 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.
   - 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.
4. Función L de una curva elíptica.
   - Reducción módulo un primo.
   - Modelo mínimo global.
   - Conductor.
   - Función L de una curva elíptica
5. Curvas elípticas sobre los complejos.
   - Retículos en $\mathbb{C}$.
   - Funciones elípticas. Función $\wp$ de Weierstrass.
   - Ecuación diferencial para $\wp$.
   - Teorema de Uniformización.
   - Cálculo del retículo de una curva elíptica.
6. Curvas modulares.
   - Construcción de $Y(1)$ y $X(1)$.
   - Grupos de congruencia.
   - Curvas modulares X_Γ.
   - Curvas modulares como espacios de moduli.
7. Formas modulares.
   - Funciones y formas modulares de nivel 1. q-expansión.
   - Formas modulares y cuspidales de nivel superior.
   - Producto escalar de Petersson. Operadores de Hecke.
   - Formas nuevas y su cuerpo de coeficientes.
   - Función L de una forma cuspidal de nivel N. Ecuación funcional.
8. Modularidad.
   - Teorema de Modularidad.
   - Parametrización modular.
   - 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.

BIBLIOGRAFÍA

- F. Diamond y J. Shurman, *A first course in modular forms*. GTM 228. *Springer-Verlag*, 2005.
- A.W. Knapp, *Elliptic Curves. Princeton University Press*, 1992.
- A. Lozano-Robledo, *Elliptic curves, modular forms, and their L-functions.* Student Mathematical Library, 58. AMS 2011.
- J.S. Milne, *Elliptic Curves*, BookSurge Publishers, 2006.
- 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.

SAGE : `http://www.sagemath.org` Magma : `http://http://magma.maths.usyd.edu.au/magma`

PROFESOR

Enrique González Jiménez, Despacho 17-508

`enrique.gonzalez.jimenez@uam.es` `http://www.uam.es/enrique.gonzalez.jimenez`
