Propuesta de Trabajos Fin de Grado
curso académico 2022-23

PROFESOR: Enrique González Jiménez

Comentario para las/los alumnos/as:Si tienes alguna duda sobre la propuesta puedes ponerte en contacto conmigo.

Número máximo de TFG que solicita dirigir: 3

1.- TÍTULO: **Teoría de géneros**

Resumen/contenido: Una forma binaria cuadrática es un polinomio de la forma $f(x,y)=ax^2+bxy+cy^2$ donde a,b y c son enteros. Gauss en Disquisitiones Arithmeticae hizo un estudio sistemático de las formas binarias cuadráticas. En particular él estaba interesado en determinar que enteros m son representados por una forma binaria cuadrática, es decir, cuando la ecuación $f(x,y)=m$ tiene solución entera. Este es el punto de partida de la Teoría de géneros. Es una de las partes más profundas desarrolladas por Gauss en Disquisitiones Arithmeticae. Este TFG consistirá en un acercamiento a esta teoría desde un lenguaje moderno.

Este TFG se enmarca dentro del Área de Álgebra. En concreto dentro de la Teoría de Números Algebraica.

Dificultad estimada: Media/Alta.

Referencia inicial:

Cox, D.A.: Primes of the form $x^2 + ny^2$, Wiley (2013).

2.-TÍTULO: **Cubos de Bhargava**

Resumen/contenido: Uno de los libros más influyentes de la historia de las matemáticas es Disquisitiones Arithmeticae que Gauss escribió en 1801. Gran parte de este libro está dedicado a estudiar formas binarias cuadráticas, en particular de definir una ley de composición entre ellas. Esta ley de composición da una estructura de grupo al conjunto de clases de equivalencia de formas binarias cuadráticas de un discriminante fijado. En 2004 Bhargava definió nuevas leyes de composición mediante *cubos*. El TFG consistirá en estudiar en un lenguaje moderno la teoría de composición de formas binarias cuadráticas hasta llegar a la reciente de Bhargava.

Este TFG se enmarca dentro del Área de Álgebra. En concreto dentro de la Teoría de Números Algebraica.

Dificultad estimada: Media/Alta (dependiendo del objetivo del alumno).

Artículo de divulgación:

François Séguin. Composition of Binary Quadratic Forms: Understanding the Approaches of Gauss, Dirichlet and Bhargava. Resonance volume 24 (2019), 633-651.

3.-TÍTULO: **Grupo de clases de ideales de ordenes en cuerpos cuadráticos**

Resumen/contenido: Sea K un cuerpo de número y O_K el anillo de enteros K. Se sabe que O_K no siempre es un dominio de factorización única. El concepto de ideal de un anillo fue introducido por Kummer y Dedekind para poder evitar esta dificultad, ya que a nivel de ideales hay factorización única en O_K. Pero decidir si O_K es un DFU no es fácil. Para ello se introduce el concepto del grupo de clases de ideales de O_K. En particular se demuestra que O_K es un DFU si es este grupo tiene cardinal 1. Este es el resumen de un curso básico de Teoría Algebraica de Números. Este TFG quiere ir un paso más, estudiando el caso en el que se sustituye el anillo O_K por lo que llamaremos un orden de K y se limitará al caso en el que K es un cuerpo cuadrático.

Este TFG se enmarca dentro del Área de Álgebra. En concreto dentro de la Teoría de Números Algebraica.

Dificultad estimada: Media/Alta (dependiendo del objetivo del alumno).

Referencia inicial:

F. Jarvis. Algebraic Number Theory. Springer (2014).

4.- TÍTULO: **Aritmética de Curvas elípticas**. Genérico.

Resumen/contenido: Las curvas elípticas son en la actualidad centrales en muchas ramas de la Teoría de Números. También en la Criptografía. Esta propuesta pretende estudiar las nociones básicas de estas curvas. Depende de los intereses del alumno se podrá centrar el objetivo.

Este TFG se enmarca dentro del Área de Álgebra. Concretamente dentro de la Teoría de Números, la Geometría Algebraica y/o la Criptografía.

Dificultad estimada: Media/Alta (dependiendo del objetivo del alumno).

Dos artículos de divulgación de La Gaceta de la RSME:

- Orientado a Teoría de Números y Geometría Algebraica:

Álvaro Lozano Robledo. Buscando puntos racionales en curvas elípticas: Métodos explícitos. Vol. 8.2 (2005), 471-488.

- Orientado a Criptografía:

José Luis Gómez Pardo. Criptografía y curvas elípticas. Vol. 5.3 (2002), 737-777.
