# Propuesta de Trabajos Fin de Grado
# curso académico 2023-24

**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: 2 + conjunto con María Inés de Frutos

---

1.-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.

Referencia inicial:

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

---

2.- TÍTULO: **Aritmética de Curvas elípticas**. Genérico. (2 alumnos)

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.