UNIVERSIDAD DE GRANADA

FACULTAD DE CIENCIAS

Propuesta TFG. Curso 2026/2027

GRADO: Grado en Matemáticas

CÓDIGO DEL TFG: 270-001-2026/2027

1. DATOS BÁSICOS DEL TFG:

Título: Aritmética de una curva elíptica

Descripción general (resumen y metodología):

Las curvas elípticas son un ejemplo de curva algebraica con varias aplicaciones en diversos campos de la matemática. Sirva como ejemplo que dichas curvas son el componente principal de la entonces Conjetura de Taniyama-Shimura que sirvió para la demostración del Último Teorema de Fermat.

Hoy en día, una de las apliaciones más utilizadas es la criptografía. La estructura de grupo que es posible definir en el conjunto de puntos de una curva elíptica puede emplearse para definir protocolos de intercambio de claves tipo Diffie-Hellman, o algoritmos de firma digital, como el estándar del NIST ECDSA.

Este TFG busca definir una aritmética en los puntos de una curva elíptica y demostrar que dicha aritmética confiere a los puntos de estructura de grupo. Por supuesto lo más complicado es demostrar la asociatividad.

Existen varias formas de hacer esa demostración. Abordaremos dos de ellas, una demostración de inspiración geométrica que utiliza el Teorema de Bezout y otra más algebraica que empleta la teoría de divisores.

Tipología: Estudio de casos, teóricos o prácticos, relacionados con la temática del Grado.

Objetivos planteados:

1. Definir el concepto de curva elíptica afín y proyectiva. Describir sus formas normales y clasificarlas en función de sus singularidades.
2. Introducir la aritmética de los puntos de una curva elíptica. Analizar el comportamoiento frente a extensiones de cuerpos.
3. Demostrar geométricamente la asociatividad de la estructira definida.
4. Demostrar algebraicamente la asociatividad de la estructura definida.

De los dos objetivos últimos se pretende abordar al menos uno de ellos. Hay un objetivo adicional y opcional en función del desarrollo del trabajo.

1. Calcular la complejidad de la aritmética de una curva elíptica en un cuerpo finito.

Bibliografía básica:

1. Lawrence C. Washington. Elliptic curves: number theory and cryptography. Second Edition. Taylor & Francis Group, 2008.
2. Andreas Enge. Elliptic curves and their application to cryptography: an introduction. Kluwe Academic Publishers, 1999.
3. Joseph H. Silverman. The Arithmetic of Elliptic Curves. Second Edition. Springer, 2009. DOI 10.1007/978-0-387-09494-6.

Recomendaciones y orientaciones para el estudiante:

Plazas: 1

2. DATOS DEL TUTOR/A:

Nombre y apellidos: FRANCISCO JAVIER LOBILLO BORRERO

Ámbito de conocimiento/Departamento: ÁLGEBRA

Correo electrónico: jlobillo@ugr.es

3. COTUTOR/A DE LA UGR (en su caso):

Nombre y apellidos:

Ámbito de conocimiento/Departamento:

Correo electrónico:

4. COTUTOR/A EXTERNO/A (en su caso):

Nombre y apellidos:

Correo electrónico:

Nombre de la empresa o institución:

Dirección postal:

Puesto del tutor en la empresa o institución:

Centro de convenio Externo:

5. DATOS DEL ESTUDIANTE:

Nombre y apellidos: JOAN DIAZ RIVERO

Correo electrónico: jdiri0805@correo.ugr.es