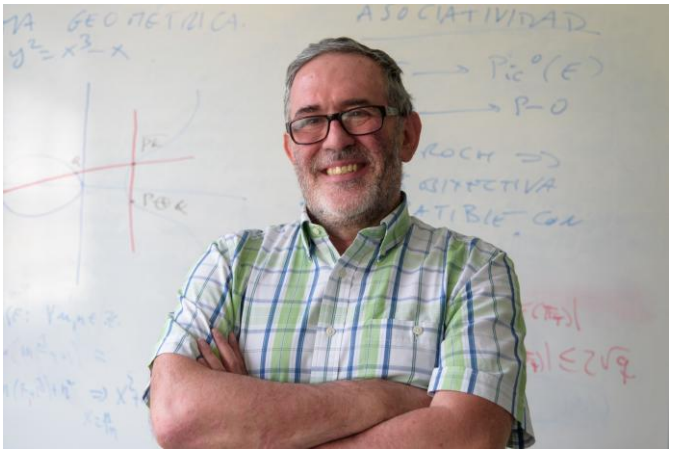
Coloquio para estudiantes

Especialmente dirigido al alumnado del Grado en Matemáticas

Curvas elípticas: de WhatsApp a la criptografía poscuántica

Adolfo Quirós Gracián
Universidad Autónoma de Madrid



Miércoles 12 de febrero de 2025, 15:30
Sala de conferencias del Módulo 00, Facultad de Ciencias

Resumen. Las curvas elípticas tienen una larga historia, en la que aparecen nombres como Fermat, Newton, Legendre, Abel, Jacobi o Weierstrass. Los polinomios que definen las curvas elípticas pueden tener coeficientes en cualquier cuerpo (por ejemplo, Z/pZ) y, demostrando una vez más el asombroso poder de las Matemáticas, en el siglo XXI las curvas elípticas definidas sobre cuerpos finitos están resultando útiles para crear protocolos seguros de criptografía de clave pública, tanto clásicos como resistentes a ataques con un ordenador cuántico. En la charla, que no asumirá conocimientos ni de curvas elípticas, ni de criptografía ni de física cuántica, presentaremos lo necesario para entender cómo se llega a estas aplicaciones. Concluiremos con un ejemplo reciente que muestra por qué la generalización y la abstracción son importantes, incluso si lo único que nos interesase de las Matemáticas fuesen las aplicaciones.

El conferenciante. Adolfo Quirós Gracián es doctor por la Universidad de Minnesota y profesor titular de Álgebra en la UAM, donde se licenció y donde coordina actualmente la especialidad de Matemáticas del Máster de Formación de Profesorado. Su investigación se enmarca en la llamada Geometría Algebraica Aritmética, lugar de encuentro de varios campos de las Matemáticas. Ha tenido un papel destacado en la Real Sociedad Matemática Española, de la que ha sido vicepresidente y donde dirige la revista para los socios, La Gaceta de la RSME. Fue vocal y presidente del Comité de Ética de la European Mathematical Society. Participa con frecuencia en actividades de divulgación, destacando entre ellas los desafíos matemáticos del diario "El País". Como reconocimiento a su labor, recibió en 2018 una de las Medallas de la Real Sociedad Matemática Española.