# ATENEO


## Adolfo Quirós Gracián

***Universidad Autónoma de Madrid***


# *Curvas elípticas y mensajes secretos: de WhatsApp a la criptografía poscuántica.*


**Abstract:** Se llama curva elíptica a una curva algebraica (proyectiva) plana, lisa y de grado 3. Estos objetos tienen una larga historia, en la que aparecen nombres como Newton, Legendre, Abel, Jacobi o Weierstrass. Los polinomios que definen las curvas elípticas pueden tener coeficientes en cualquier cuerpo, y a lo largo del siglo XX se estudiaron en profundidad sus propiedades aritméticas, estudio en el que Fermat fue pionero. En un interesante giro de guion, la aritmética (profunda) de las curvas elípticas resultó fundamental en la prueba por Wiles del Último Teorema de Fermat. 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.


**Sala de Grados I, Facultad de Ciencias**
**Jueves 9 de Mayo de 2024 (17:00)**