



FACULTAD DE CIENCIAS

CURSO DE POSTGRADO

Nombre del curso	Curvas Elípticas
Tipo de curso (Obligatorio, Electivo, Seminario)	Electivo
N° de horas totales (Presenciales + No presenciales)	216 horas
N° de Créditos	8 SCT
Fecha de Inicio – Término	Marzo – Julio 2025
Días / Horario	Por definir
Lugar donde se imparte	Departamento de Matemática y Ciencia de la Computación, Facultad de Ciencia, Universidad de Santiago de Chile.
Profesor Coordinador del curso	Giancarlo Lucchini
Profesores Colaboradores o Invitados	David Grimm y Sebastián Herrero (USACH)
Descripción del curso	Iniciaremos con la teoría de curvas algebraicas siguiendo el libro de Fulton. En particular, se presentará el teorema de Bézout sobre la intersección de curvas de un grado dado para definir la operación de grupo en una curva elíptica. Luego, siguiendo el libro de Silverman, profundizaremos en el estudio de éstas. Si el tiempo lo permite, profundizaremos en la teoría de curvas elípticas sobre C , sobre Q y sobre cuerpos finitos.
Objetivos	Este curso puede ser un punto de partida para una tesis en Ingeniería Matemática (explorando aspectos computacionales de curvas elípticas sobre cuerpos finitos), o una tesis de posgrado en teoría de números.
Contenidos	Variedades afines y proyectivas, propiedades locales (puntos suaves, clasificar singularidades, multiplicidad de intersecciones). Teorema de Bézout sobre intersección de curvas. Curvas elípticas y sus modelos de Weierstrass. Operación de grupo en curvas elípticas, isogenias entre curvas elípticas. Curvas elípticas sobre C , Q y cuerpos finitos.
Modalidad de evaluación	Entregas de ejercicios (60%) y una exposición (40%).

Bibliografía	Obligatoria: W. Fulton. <i>Algebraic Curves</i> . J. Silverman. <i>The Arithmetic of Elliptic Curves</i> . Q. Liu. <i>Algebraic Geometry and Arithmetic Curves</i> .