Curvas Elípticas - Electivo 1er semestre 2025

Prerequisitos: Álgebra abstracta (grupos, anillos), Topología.

Docentes: David Grimm, Sebastián Herrero.

Motivación: La teoría de curvas algebraicas tiene un rol distinguido dentro de la geometría algebraica, ya que permiten el uso de muchas más herramientas que en variedades de dimensión superior. Entre las curvas algebraicas, las curvas elípticas (curvas suaves de género 1) forman una categoría especial. Ellas pueden ser descritas por el conjunto de soluciones de una ecuación polinomial $f(x, y) = 0$ de grado 3 en 2 variables. Las soluciones racionales de esa ecuación (puntos racionales) pueden ser combinadas a travéz de una operación de grupo. Eso las hace objetos interesantes para la Matemática pura al igual que para la Criptografía: Muchos problemas de la teoría de números que en primera vista no tienen nada que ver con curvas elípticas permiten conexiones escondidas con ellas, lo que permite convertir el problema original en un problema sobre existencia de curvas elípticas con ciertas propiedades o existencia de ciertos puntos racionales en una curva elíptica. El ejemplo más conocido es el último teorema de Fermat, pero hay muchos ejemplos más. Por otro lado, curvas elípticas sobre cuerpos finitos son una fuente abundante de grupos cíclicos finitos, donde el así llamado "problema del logaritmo discreto" es computacionalmente más difícil de resolver que para otras fuentes de tales grupos. Eso las hace objetos preferidos para implementar protocolos de criptografía.

Contenido: Iniciaremos con la teoría de curvas algebraicas siguiendo el libro de Fulton, estudiando variedades afines y proyectivas, y algunas de sus propiedades locales (como puntos suaves, clasificar singularidades, multiplicidad de intersecciones). En particular, se presentará el teorema de Bézout sobre la intersección de curvas de un grado dado, lo que se puede utilizar entre otros en la definición de operación de grupo en una curva elíptica. Luego, siguiendo el libro de Silverman, profundizaremos en el estudio de curvas elípticas y sus modelos de Weierstrass, su estructura de grupo e isogenias entre distintas curvas elípticas. Si el tiempo lo permite, profundizaremos en la teoría de curvas elípticas sobre $\mathbb{C}$, sobre $\mathbb{Q}$ y sobre cuerpos finitos.

Para aspectos de la teoría de cuerpos que se van a utilizar, pero que no se han visto en un curso de Álgebra abstracta de pregrado, se proporcionarán guías de autoestudio que acompañarán resúmenes breves de estos temas en el curso.

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.

Evaluación: Entregas de ejercicios (60 %) y una exposición (40 %).

Horarios: Por definir.

Contacto : david.grimm@usach.cl, sebastian.herrero@usach.cl.

Bibliografía:

- W. Fulton, "Algebraic Curves" (`https://dept.math.lsa.umich.edu/~wfulton/CurveBook.pdf`)
- J. Silverman, "The Arithmetic of Elliptic Curves".
- Q. Liu, " Algebraic Geometry and Arithmetic Curves".