Proyecto de trabajos de fin de grado ofrecido por
Angélica Benito Sualdea
2016-17

1) **Introducción a la Geometría Algebraica y a las Singularidades**.

Resumen: En este trabajo exploraremos las bases de la geometría algebraica revisando las nociones de variedad algebraica, la definición de la topología de Zariski, la relación entre el álgebra y la geometría (Teorema de los ceros de Hilbert), la noción de dimensión... así como el principal objetivo del trabajo: la definición de lisitud, de singularidad, y el criterio Jacobiano. En esta línea, trataremos de entender el problema de resolución de singularidades, así como la herramienta principal usada en la demostración de este problema (en característica cero): las explosiones.

Requisitos: es recomendable cursar la asignatura de Álgebra Conmutativa durante el año en el que se realice el trabajo y haber cursado la Teoría de Galois.
Referencias:
- M.F. Atiyah, I.G. Macdonald, Introducción al Álgebra Conmutativa, ed. Reverté. Última edición de 2010.
- M. Reid, Undergraduate Algebraic Geometry, London Mathematical Society, Student Texts 12, 1998, Cambridge University Press.
- M. Reid, Undergraduate Commutative Algebra, London Mathematical Society, Student Texts 29, 2002, Cambridge University Press.
- S.D. Cutkosky, Resolution of singularities, Graduated Studies in Mathematics, volume 63, 2004, American Mathematical Society.
- K. E. Smith, Karen, L. Kahanpää, P. Kekäläinen, W. Traves, William, An invitation to algebraic geometry, Universitext. Springer-Verlag, New York, 2000.

2) **El problema del logaritmo discreto y sus aplicaciones a la Criptografía**.

Resumen: En nuestros primeros pasos en matemáticas aprendemos reglas sobre exponenciación (de números reales) y lo sencillo que es calcular la inversa de este proceso usando logaritmos en la base correspondiente. Pero, ¿qué pasa cuando exponenciamos sobre otros cuerpos? Más aún, ¿qué sucede cuando consideramos la exponenciación sobre cuerpos finitos? En este trabajo veremos que el proceso se puede volver especialmente caótico y complicado (no es fácil calcular logaritmos) y que este hecho nos abre las puertas a múltiples aplicaciones en la criptografía (firma digital, criptosistema ElGamal). El objetivo será ver la complejidad de este problema, las ventajas e inconvenientes de su uso en relación a otros métodos de cifrado, así como posibles formas de implementarlo (por ejemplo, usando curvas elípticas).
Requisitos: Tener un cierto bagaje en asignaturas de álgebra, por lo que es recomendable (aunque no indispensable) haber cursado la Teoría de Galois.
Referencias:
- S. D. Galbraith. Mathematics of Public Key Cryptography, Cambridge University Press (2012)
- J. Katz, Y. Lindell, Introduction to Modern Cryptography, Chapman & Hall/CRC, 2008.
- N. Koblitz, A Course in Number Theory and Cryptography, Graduate Texts in mathematics 114, 1987, Springer-Verlag.
- I. Shparlinski, Number Theoretic Methods in Cryptography, Progress in Computer Science and Applied Logic 17, 1999, Birkhäuser Basel.