

Propuesta de Trabajos Fin de Grado, curso académico 2021-22

PROFESOR: Daniel Ortega Rodrigo

Número máximo de TFG que solicita dirigir: 3 (contando con los compartidos)

1.- TEMA: Polinomios irreducibles sobre cuerpos finitos

Válido para 1 alumno.

Resumen/contenido:

La aritmética en cuerpos finitos es una herramienta de plena actualidad, de uso en, por ejemplo, teoría de códigos y criptografía. Para realizar operaciones en cuerpos finitos se necesitan construir polinomios irreducibles. Esta tarea no es demasiado costosa para cuerpos de característica pequeña, en los que se suele acudir a los polinomios de Conway, que aportan una notación estándar para extensiones de cuerpos. Pero para cuerpos de característica no tan pequeña, es costoso encontrar polinomios de Conway, incluso en grados bajos. Así, encontrar polinomios irreducibles en cuerpos finitos es aún una tarea de interés.

En este trabajo se ofrece estudiar los algoritmos actuales en este campo.

Requisitos: Conocimientos básicos de álgebra abstracta y cierto gusto por la programación (preferiblemente conocimientos de Sagemath).

Asignaturas de cuarto relacionadas/compatibles:

Bibliografía/referencias:

- Adleman, L. M., and Lenstra, H. W., Jr.: "Finding irreducible polynomials over finite fields", in Proc 18th Annual ACM Sympos. On Theory of Computing, 1986, pp. 350–355.
- Berlekamp, E. ; "Factoring polynomials over large finite fields". Math. Comp. 24 (1970), pp. 713–735.
- Shoup, V.: "New algorithms for finding irreducible polynomials over finite fields". Math. Comp. 54 (1990), no. 189, 435–447.
- Sugimoto, E.: "A short note on new indexing polynomials of finite fields". Inform. and Control 41 (1979), no. 2, 243–246.