Propuesta de Trabajos Fin de Grado, curso académico 2022-23

PROFESOR/A: Adolfo Quirós Gracián

Número máximo de TFG que solicita dirigir: 2

1.- **TÍTULO**: EL FACTORIAL DE BHARGAVA

Resumen/contenido: En 1996 Manjul Bhargava propuso una generalización del factorial de un entero que le permitió dar una respuesta completa a una pregunta interesante sobre los valores que toman los polinomios con coeficientes enteros (la versión "estándar" dice: si f es un polinomio primitivo con coeficientes enteros de grado k, entonces el máximo común divisor de todos los valores f(n), n entero, divide a k!). Lo hizo usando unas nuevas herramientas llamadas p-ordenaciones, en principio elementales, pero que en sus manos dieron estupendos frutos. El trabajo a desarrollar consistiría en entender los factoriales de Bhargava, sus aplicaciones y, en su caso, algunas de sus extensiones (a anillos de Dedekind, a varias variables,...).

Bibliografía/referencias:

- M. Bhargava, The factorial function and generalizations. *Amer. Math. Monthly* **107** (2000), no. 9, 783–799.
- M. Bhargava, Generalized factorials and fixed divisors over subsets of a Dedekind domain. *J. Number Theory* **72** (1998), no. 1, 67–75.
- P.-J. Cahen,J.-L. Chabert, K. S. Kedlaya, Bhargava's early work: the genesis of P-orderings. *Amer. Math. Monthly* **124** (2017), no. 9, 773–790.
- S. Evrard, Bhargava's factorials in several variables. *J. Algebra* **372** (2012), 134–148.

Válido para más de un estudiante: NO

2.- **TÍTULO**: TEORÍA DE GALOIS, DESCOMPOSICIÓN Y DISTRIBUCIÓN DE IDEALES EN ANILLOS DE NÚMEROS

Resumen/contenido: El objetivo del trabajo es ir más allá de lo que se suele cubrir en el curso de Teoría Algebraica de Números, estudiando cuestiones como el efecto de la acción del grupo de Galois sobre la descomposición en ideales primos o como se distribuyen los ideales entre las distintas clases del grupo de clases. Se trata en principio de cubrir los capítulos 4, 6 y 7 del libro de Marcus e, idealmente, de estudiar algo de teoría de cuerpos de clase para poder entender también el contenido del capítulo 8 (que tiene pocos detalles). Nota: este trabajo requiere conocimientos de Teoría de Galois y Teoría Algebraica de Números.

Bibliografía/referencias:

- Daniel A. Marcus, *Number Fields* (2nd ed). Springer (2018)
- David A. Cox . *Primes of the form x^2+ny^2* (2nd ed). Wiley (2013)

Válido para más de un estudiante: NO

3- **TÍTULO**: TEORÍA DE GALOIS: MÁS ALLÁ DE LAS EXTENSIONES FINITAS DE Q

Resumen/contenido: El objetivo del trabajo es estudiar algunas cuestiones sobre extensiones de cuerpos que no suelen cubrirse en el curso básico sobre Teoría de Galois, en particular, las distintas caracterizaciones de las extensiones separables, el teorema de Galois para extensiones infinitas o el grupo de Galois absoluto de un cuerpo finito. Dependiendo del tiempo, se puede estudiar también otros temas, como la teoría de descenso o las extensiones abelianas.

Bibliografía/referencias:

- K. Conrad. Varios documentos disponibles en su web: https://kconrad.math.uconn.edu/blurbs/
- N. Jacobson, *Basic Algebra II* (2nd ed), W. H. Freeman & Co., 1989. (Capítulo 8)
- A. W. Knapp, Advanced Algebra, Birkhäuser, 2007 (Capítulo 7)

Válido para más de un estudiante: NO

4- **TÍTULO**: CURVAS ELÍPTICAS, FUNCIONES L Y APLICACIONES

Resumen/contenido: Entre los muchos problemas que Pierre de Fermat estudió, estaban el de los números congruentes (¿qué números racionales son áreas de triángulos rectángulos con lados racionales?) y el de encontrar soluciones enteras a ecuaciones de la forma x^n+y^n=z^n (la no existencia de soluciones no triviales para n>2 es el conocido como "último teorema"). Quizás sorprendentemente, ambos problemas se han resuelto utilizando curvas elípticas, las funciones L que se les asocian, y la relación de estas con las formas modulares, todo ello a través de resultados y conjeturas como la de Shimura-Taniyama-Weil (ahora teorema de Wiles) o la de Birch y Swinnerton-Dyer (uno de los problemas del milenio). El objetivo propuesto para el TFG es estudiar las propiedades básicas de estos objetos y las relaciones entre ellos.

Bibliografía/referencias:

- K. Conrad, The congruent number problem, *Harvard College Mathematical Review*, **2** (2) (2013), 58–73.
- F.Q. Gouvêa, A marvelous proof, *Amer. Math. Monthly* **101** (1994), no. 3, 203-222.
- A. W. Knapp. *Elliptic Curves* ,Princeton University Press, 1992.
- N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer, 1993.
- A. Lozano-Robledo, *Elliptic Curves, Modular Forms, and Their L-functions*, AMS, 2011.

Válido para más de un estudiante: SÍ (tras una parte común, se puede tratar por un lado el problema de los números congruentes y por otro el último teorema de Fermat).

5.- **TÍTULO**: CRIPTOGRAFÍA BASADA EN EMPAREJAMIENTOS

Resumen/contenido: Los emparejamientos (en grupos) se han convertido en los últimos años en una poderosa herramienta criptográfica. Tienen aplicaciones como

el intercambio tripartitos de claves, las firmas cortas o la criptografía basada en la identidad, y también, desde un punto de vista distinto, permiten atacar el problema del logaritmo discreto en algunas curvas elípticas. El trabajo a desarrollar tendría dos partes. Por una parte, la descripción de algunas de estas aplicaciones. Por otra, la construcción del emparejamiento de Weil para curvas elípticas.

Bibliografía/referencias:

- R.Dutta, R. Barua, P. Sarkar, *Pairing-Based Cryptographic Protocols: A Survey*. Cryptology ePrint Archive: Report 2004/064: https://eprint.iacr.org/2004/064.pdf

- S. D. Galbraith, K. G.Paterson, N. P.Smart, Pairings for cryptographers. *Discrete Applied Mathematics* **6** (2008.), 3113-3121

- A. Menezes, An Introduction to Pairing-Based Cryptography, en I. Luengo (ed.), *Recent Trends in Cryptography, Contemporary Mathematics* **477** (2009), 47-65. Disponible en la web del autor: https://www.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf

- K.G. Paterson, *Cryptography from Pairings*. Capítulo X de I. F. Blake, G. Seroussi, N. P. Smart (eds.), *Advances in Elliptic Curve Cryptography*, Cambridge U. P. (2009)

- J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Springer, 2009.

Válido para más de un estudiante: NO

6.- **TÍTULO**: APLICACIONES DE LOS RETÍCULOS EN CRIPTOGRAFÍA

Resumen/contenido: El primer uso de los retículos en criptografía fue un ataque al protocolo de clave pública basado en el problema de la mochila (*knapsack problem*) que habían propuesto Merkle y Hellman en 1978. Posteriormente han aparecido otros, como el uso del método de Coppersmith para atacar claves RSA con conocimiento parcial de un factor o el criptosistema de Goldreich-Goldwasser-Halevi, hasta llegar a las propuestas de criptografía poscuántica basadas en el "Aprendizaje con Errores". El objetivo del TFG es entender los problemas básicos sobre retículos en los que se basan estas aplicaciones y estudiar algunas de ellas

Bibliografía/referencias:

- C. Costello, Post-quantum key exchange for the Internet based on lattices (2016), https://static1.squarespace.com/static/5fdbb09f31d71c1227082339/t/5ff379814688fd421b7a05b2/1609791877407/2016-MSRIndiainvitedtalk.pdf

- S. D. Galbraith, *Mathematics of Public Key Cryptography* (2012), Parte IV. Disponible en la web del autor: https://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html

- D. Micciancio, O. Regev, *Lattice-based Cryptography*. Capítulo de *Post-quantum Cryptography*, D. J. Bernstein and J. Buchmann (eds.), Springer (2008). https://link.springer.com/content/pdf/10.1007%2F978-3-540-88702-7_5

- O. Regev, *The Learning with Errors Problem*. Disponible en la web del autor: https://cims.nyu.edu/~regev/papers/lwesurvey.pdf

Válido para más de un estudiante: SI (podrían hacerlo 2 estudiantes estudiando distintas aplicaciones)