Propuesta de Trabajos Fin de Grado, curso académico 2023-24

PROFESOR: ADOLFO QUIRÓS GRACIÁN

Número máximo de TFG que solicita dirigir: 2

1.- TEMA: EL FACTORIAL DE BHARGAVA

Válido para 1 alumno.

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,...).

Requisitos: Estructuras algebraicas, Matemática discreta

Asignaturas de cuarto relacionadas/compatibles: Teoría de Números

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.

2.- TEMA: ANILLOS DE ENTEROS DE CUERPOS DE NÚMEROS

Válido para 2 alumnos.

Resumen/contenido: El objetivo es “demostrar algunos de los principales teoremas de la asignatura Teoría Algebraica de Números (no ofertada en 2023-2024)”. En concreto, se quiere entender la factorización de ideales en el anillo de enteros de un cuerpo de números, el grupo de clases de ideales, quizás el teorema de las unidades (el origen de este estudio está en los intentos de demostrar el Último Teorema de Fermat). Se propone para más de un estudiante porque, aparte de los resultados comunes, se puede optar por centrarse en los cuerpos cuadráticos o en los ciclotómicos

Requisitos: Estructuras algebraicas. Sería útil conocer las extensiones de cuerpos (que se dan en Teoría de Galois).

Asignaturas de cuarto relacionadas/compatibles: Teoría de Números, Teoría de Galois.

Bibliografía/referencias:

- D. A. Marcus, *Number Fields*, 2ª ed., Springer, 2018.
- F. Jarvis, Algebraic Number Theory, Springer, 2014.

- Stewart, D. O. Tall, Algebraic number theory and Fermat's last theorem, 3ª ed., , A. K .Peter, 2002

3.- TEMA: EL TEOREMA FUNDAMENTAL DEL ÁLGEBRA

Válido para 2 alumnos.

Resumen/contenido: El objetivo del trabajo es presentar y comprender varias demostraciones del Teorema Fundamental del Álgebra, desde la original de Gauss en términos de polinomios reales a las que usan topología, geometría, variable compleja, multiplicadores de Lagrange, teoría de Galois, análisis no estándar.... (se puede elegir presentar unas u otras en función de los intereses). Es interesante que nada menos que Leibniz "demostró" que el teorema era falso (el trabajo podría incorporar algunas referencias históricas).

Requisitos: Estructuras Algebraicas, Variable compleja I, Topología, Teoría de Galois, ... (los requisitos dependen de las demostraciones que se incluyan)

Asignaturas de cuarto relacionadas/compatibles: Ninguna en especial.

Bibliografía/referencias:

- R. P. Boas, Jr. A Proof of the Fundamental Theorem of Algebra. *The American Mathematical Monthly*. Vol. 42, No. 8 (Oct. 1935), 501-502
- D. Girela, Una demostración del Teorema Fundamental del Álgebra, *La Gaceta de la RSME* 21, no. 2 (2018), 258.
- T. de Jong. Lagrange Multipliers and the Fundamental Theorem of Algebra. *The American Mathematical Monthly*, Vol. 116, No. 9 (Nov. 2009), 828-830
- G. Leibman. A Nonstandard Proof of the Fundamental Theorem of Algebra. *The American Mathematical Monthly*, Vol. 112, No. 8 (Oct. 2005), 705-712
- O. Rio Branco de Oliveira. The Fundamental Theorem of Algebra: An Elementary and Direct Proof. *The Mathematical Intelligencer*. Volume 33, Issue 2 (July 2011), 1–2

4.- TEMA: ÁLGEBRA Y CÓDIGOS NEURONALES

Válido para 1 alumno.

Resumen/contenido: Los códigos neuronales son un modelo del funcionamiento de las células del sistema nervioso. Un código neuronal se define como las combinaciones de neuronas activadas en respuesta a un determinado conjunto de estímulos. Existen diversos puntos de vista al abordar el estudio de los códigos neuronales. La propuesta es seguir la línea propuesta por Carina Curto, Vladimir Itskov, Alan Veliz-Cuba y Nora Youngs, y estudiar los códigos neuronales utilizando herramientas de álgebra conmutativa: los anillos y los ideales neuronales.

Requisitos: Estructuras algebraicas, Matemática discreta.

Asignaturas de cuarto relacionadas/compatibles: Álgebra Conmutativa.

Bibliografía/referencias:

- C. Curto, V. Itskov, A. Veliz-Cuba, N. E. Youngs. The neural ring: An algebraic tool for analyzing the intrinsic structure of neural codes. Bulletin of Mathematical Biology 75 (2013), 1571-1611.
- N. R. Youngs. The neural ring: Using algebraic geometry to analyze neural codes. Tesis doctoral, Universidad de Nebraska-Lincoln (2014). https://digitalcommons.unl.edu/mathstudent/56.

- D. Cox, J. Little, D. O'Shea. Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra. Springer (2015).

5.- TEMA: CRIPTOGRAFÍA BASADA EN EMPAREJAMIENTOS

Válido para 1 alumno.

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.

Requisitos: Estructuras algebraicas.

Asignaturas de cuarto relacionadas/compatibles: Teoría de Códigos y Criptografía.

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.

6.- TEMA: UN EJEMPLO DE CRIPTOGRAFÍA POSCUÁNTICA: LA CRIPTOGRAFÍA BASADA EN CÓDIGOS

Válido para 1 alumno.

Resumen/contenido: L En 1994 Peter Shor propuso un algoritmo cuántico que obligará a abandonar los actuales criptosistemas de clave pública (RSA o El Gamal) el día que el ordenador cuántico se haga realidad. Es por tanto importante contar con criptosistemas de clave pública cuya seguridad no dependa de problemas que podrá resolver un ordenador cuántico. Es la llamada criptografía poscuántica. En el trabajo, además del problema general, se estudiará un ejemplo de estos criptosistemas, los basados en técnicas de códigos correctores, en particular el de McEliece, que es la base de uno de los protocolos que el NIST de EEUU está considerando como posble estándar poscuántico (https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4)

Requisitos: Álgebra Lineal, Estructuras algebraicas.

Asignaturas de cuarto relacionadas/compatibles: Teoría de Códigos y Criptografía.

Bibliografía/referencias:

- S. Au, C. Eubanks-Turner, J. Everson. *The McEliece Cryptosystem*. Manuscrito no publicado, 2013 (http://www.math.unl.edu/~s- jeverso2/McElieceProject.pdf)
- D. Bernstein. Introduction to post-quantum cryptography. En D. Bernstein, J. Buchmann, E. Dahmen (eds), *Post-Quantum Cryptography*, Springer, 2009 (https://pqcrypto.org/www.springer.com/cda/content/document/cda_download documen t/9783540887010-c1.pdf)
- D. Bernstein, T. Lange. *Post-quantum cryptography–dealing with the fallout of physics success*. Cryptology ePrint Archive: Report 2017/314 (https://eprint.iacr.org/2017/314/20170414:165615).
- T. Lange. *Code-based cryptography*. Charla en las Jornadas de Criptografía / Spanish Cryptography Days, Murcia 2011 (https://www.hyperelliptic.org/tanja/vortraege/murcia.ps)
- Mucha más información en la web del proyecto “Classic McEliece”. https://classic.mceliece.org/index.html