Propuesta de Trabajos Fin de Grado, curso académico 2020-21

PROFESOR/A: Adolfo Quirós Gracián

Número máximo de TFG que solicita dirigir: 3

1.- **TÍTULO**: LAS CONJETURAS DE WEIL (contenido "cerrado")

Resumen/contenido: Se llama variedad algebraica al conjunto de ceros de una familia de polinomios. Si los polinomios tienen coeficientes en un cuerpo finito, F_q el conjunto de soluciones en el cuerpo, y también en todas sus extensiones finitas F_{q^n}, es finito. Llamando N_n al cardinal de las soluciones en F_{q^n}, resulta que todos estos N_n se pueden utilizar para definir una "función zeta de la variedad" que tiene propiedades análogas a la de la función zeta de Riemann. En particular, hay un análogo de la "hipótesis de Riemann", cuya demostración general por Deligne es uno de los hitos de las matemáticas del siglo XX. El objetivo del trabajo es entender qué dicen estas propiedades, que son las llamadas Conjeturas de Weil, y demostrarlas en el caso de curvas.

Bibliografía/referencias:

- M. Hindry, La preuve par André Weil de l'hypothèse de Riemann pour une courbe sur un corps fini. En *Henri Cartan & André Weil, mathématiciens du XXe siècle*, 63-98, Ed. Éc. Polytech., Palaiseau, 2012.
- M. Mustata, *Zeta functions in algebraic geometry*. Disponible en la web del autor http://www-personal.umich.edu/~mmustata/zeta_book.pdf.
- A. Weil, Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.* **55** (1949). 497-508.

Válido para más de un estudiante: NO

2.- **TÍTULO**: CURVAS ALGEBRAICAS PLANAS (contenido "cerrado")

Resumen/contenido: La Geometría Algebraica estudia las variedades definidas por la anulación de una familia de polinomios. El caso más sencillo son las curvas algebraicas plana. El objeto del trabajo es entender algunos principios de la geometría de estas curvas. En particular, se estudiarán los teoremas de Bezout (¿en cuántos puntos, contados adecuadamente, se cortan dos curvas algebraicas planas?) y de Cayley-Bacharach (¿cuántas condiciones podemos imponer a la intersección de dos cúbicas planas?), sus antecedentes y algunas de sus consecuencias.

Bibliografía/referencias:

- E. Brieskorn, H. Knörrer, *Plane Algebraic Curves*, Birkhäuser , 1986
- A. Ding, Plane Algebraic Curves, https://staff.math.su.se/shapiro/UIUC/DingPlaneCurves.pdf
- G. Fischer, *Plane Algebraic Curves*, Student mathematical library **15**, AMS, 2001.

- W. Fulton, *Algebraic curves : an introduction to algebraic geometry*, Addison-Wesley, 1989. Disponible en la web del autor: http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

Válido para más de un estudiante: NO

3.- **TÍTULO**: EL PROBLEMA DEL LOGARITMO DISCRETO EN CRIPTOGRAFÍA (contenido "cerrado")

Resumen/contenido: Sea G=<g> un grupo cíclico. Se llama problema del logaritmo discreto en G a, dado x en G, encontrar n tal que $x=g^n$. Dependiendo de quién sea G este problema es fácil o muy difícil de resolver y, en el segundo caso, tiene múltiples aplicaciones criptográficas. El objetivo del trabajo es entender algunos de los ataques (genéricos o dependiendo de G) para resolver el problema y algunas de sus aplicaciones, como las firmas digitales o el uso que hace WhatsApp de las curvas elípticas. Dependiendo de los interés de quien lo escriba, este trabajo podría tener una componente computacional.

Bibliografía/referencias:

- D. J. Bernstein, Curve25519: new Diffie-Hellman speed records. *Proceedings of PKC 2006, LNCS 395*8, Springer, 2006, pp. 207-228. Disponible en https://cr.yp.to/ecdh/curve25519-20060209.pdf
- S. D. Galbraith , *Mathematics of Public Key Cryptography*, Cambridge U. Press, 2012. Disponible en la web del autor: https://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html

Válido para más de un estudiante: NO

4.- **TÍTULO**: TEORÍA DE GALOIS: MÁS ALLÁ DE LAS EXTENSIONES FINITAS DE Q (contenido "cerrado")

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* (2ª ed), W. H. Freeman & Co., 1989. (Capítulo 8)

Válido para más de un estudiante: NO

5- **TÍTULO**: EL TEOREMA FUNDAMENTAL DEL ÁLGEBRA (contenido "cerrado")

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.... Es interesante que nada menos que Leibniz "demostró" que el teorema era falso (el trabajo podría incorporar algunas referencias históricas).

Bibliografía/referencias (Algunas demostraciones. Las que se incluyan finalmente en el trabajo dependerán de los intereses de quien lo escriba.) :

- 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

Válido para más de un estudiante: NO

6- **TÍTULO**: SUDOKUS Y MATEMÁTICAS (contenido "cerrado")

Resumen/contenido: En cuanto se medita un momento se da uno cuenta de que, aunque aparezcan números, un sudokzle aritmético. En realidad es un puzle de teoría de grafos: consiste en colorear, usando 9 colores, un grafo con 81 vértices y 810 aristas. De ahí surgen cuestiones interesantes (¿cuántos sudokus distintos hay?, ¿cuántas pistas se necesitan para resolverlos?) que se pueden atacar con herramientas como los grupos y la teoría de grafos. También se puede "jugar" a construir sudokus con estructura matemática adicional. Estudiar algunos de estos asuntos es el objetivo del trabajo que, dependiendo de los intereses de quien lo escriba, podría tener una componente computacional.

Bibliografía/referencias:

- A. M. Herzberg, M. Ram Murty, Sudoku Squares and Chromatic Polynomials, *Notices of the AMS* **54**, no. 6 (2007), 708-717.
- K. Hossner Boden, M. B. Ward A New Class of Cayley- Sudoku Tables, *Mathematics Magazine* **9**2, no. 4 (2019), 243-251,

Válido para más de un estudiante: NO

Indicaciones:

- Podéis añadir cuantas propuestas queráis, aunque se recomienda que no sean más de 4.
- En el resumen del proyecto utilizad solo texto plano evitando en la medida de lo posible fórmulas y símbolos. La descripción debe ser breve; se sugiere una extensión no superior a 3 ó 4 líneas.
- El número máximo de TFG a dirigir por cada profesor sigue siendo 3 aunque este año no se asignará el tercero hasta que el resto de los colegas no tengan al menos 1 asignado.