Propuesta de Trabajos Fin de Grado, curso académico 2019-20

PROFESOR/A: Adolfo Quirós

1.- **TÍTULO**: LOS NÚMEROS P-ÁDICOS Y EL TEOREMA DE HASSE-MINKOWSKI

Resumen/contenido: El valor absoluto usual no es el único del que podemos dotar a los números racionales. Hay otros, llamados p-ádicos (uno para cada primo p), que tienen un sabor más aritmético. Los números p-adicos son el completado de Q respecto a estos valores absolutos, igual que los reales lo son respecto a la norma usual. Los p-ádicos, así como la versión p-ádica de los números complejos, tienen interesantes propiedades topológicas, algebraicas y analíticas. El objetivo de este trabajo es estudiar algunas de ellas y, en particular, demostrar el Teorema de Hasse-Minkowski: una forma cuadrática con coeficientes racionales tiene un cero racional si y sólo si los tienes reales y p-ádicos (para todo p).

Bibliografía/referencias:

- Z.I. Borevich.- I.R Shafarevich, *Number Theory,* Academic Press , 1966.
- F. Q. Gouvêa, *p-adic numbers: an introduction* (2nd ed.), Springer, 1997.
- S. Katok, *p-adic analysis compared with real*, Student Mathematical Library, vol. 37, American Mathematical Society, 2007.
- N. Koblitz. *p-adic numbers, p-adic analysis and zeta functions* (2nd ed.), Springer, 1984.

2.- **TÍTULO**: LAS CONJETURAS DE WEIL

Resumen/contenido: Se llama variedad algebraica al conjunto de soluciones de una familia de polinomios. Si los polinomios en cuestión 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. Si llamamos 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*, (http://www-personal.umich.edu/~mmustata/zeta_book.pdf).
- Weil, Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.* **55** (1949). 497-508.

3.- **TÍTULO**: CURVAS ELÍPTICAS, PRIMALIDAD Y FACTORIZACIÓN

Resumen/contenido: Entre las muchas aplicaciones de las curvas elípticas se encuentran un test de primalidad, propuesto originalmente por Atkin, y el algoritmo de factorización de Lenstra. El primero es en la práctica el test de primalidad más rápido para números sin características especiales y el segundo tiene la ventaja de que su eficacia depende del tamaño del factor a encontrar, y no del número a factorizar. En el trabajo se estudiará lo suficiente sobre curvas elípticas y algoritmos de primalidad y factorización como para llegar a entender los de Atkin y Lenstra. Si hubiese interes, se podrían implementar en Sage.

Bibliografía/referencias:

- H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1993.
- R. Crandall and C. Pomerance. *Prime Numbers: A Computational Perspective* (2nd ed.), Springer, 2001.
- N. Koblitz. *A course in number theory and cryptography* (2nd ed.), Springer, 1994.
- H. W. Lenstra Jr., Factoring integers with elliptic curves, *Annals of Mathematics* **126** (1987), 649–673.
- J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves* (2nd ed.), Springer, 2005.

4.- **TÍTULO**: LOS CÓDIGOS GEOMÉTRICOS DE GOPPA: PUNTO DE ENCUENTRO ENTRE LA CORRECCIÓN DE ERRORES Y LA GEOMETRÍA ALGEBRAICA

Resumen/contenido: Los códigos geométricos de Goppa utilizan las curvas algebraicas sobre cuerpos finitos para detectar y corregir errores. De hecho la existencia de curvas con muchos puntos permite definir códigos con alta capacidad de corrección y tasas de transmisión elevadas.. Además, la elección de curvas con buenas propiedades proporciona algoritmos eficaces de codificación y decodificación. El objetivo del trabajo propuesto es entender esta interacción entre curvas algebraicas y códigos correctores, para lo que habrá que estudiar algunos resultados básicos sobre curvas algebraicas (incluido el enunciado del Teorema de Rieman-Roch y resultados sobre número de puntos de curvas algebraicas sobre cuerpos finitos), así como las principales cotas de la teoría de códigos.

Bibliografía/referencias:

- V. D. Goppa, Codes and information. *Russian Math.Surveys* **39** (1984), 87-141.
- O. Pretzel, *Codes and algebraic curves*. Oxford University Press, 1998.
- T. Høholdt, J. H. van Lint, R Pellikaan, Algebraic geometry codes. En *Handbook of Coding Theory*, vol I, 871-961, Elsevier, Amsterdam 1998.

• M. A. Tsfasman, S. G. Vladut, *Algebraic-Geometric Codes*. Kluwer, Dordrecht, 1991.

• J. H. Van Lint, G. Van der Geer, *Introduction to Coding Theory and Algebraic Geometry*. Birkhäuser Verlag, Basel, 1988.

5- **TÍTULO**: EL TEOREMA FUNDAMENTAL DEL ÁLGEBRA

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

6- **TÍTULO**: LOS MÉTODOS DE REPARTO PROPORCIONAL: UNA PERSPECTIVA HISTÓRICA Y MATEMÁTICA

Resumen/contenido: La aparición de los parlamentos democráticamente elegidos planteó el problema de cómo representar mejor los intereses de la población. En unos casos se opta por la representación directa por un diputado, y en otros por una representación proporcional. Incluso en el primer caso, surge a veces la necesidad de asignar proporcionalmente los diputados a elegir en cada territorio. El objetivo del trabajo es estudiar algunas de las matemáticas que hay detrás del reparto proporcional y que han ido surgiendo a lo largo del tiempo. Entre ellas pueden estar la Paradoja de Alabama, el análisis procedimiento propuesto por Charles L. Dodgson (autor, bajo el seudónimo Lewis Carroll, de *Alicia en el país de las maravillas*), las medidas "de injusticia" o los Teoremas de imposibilidad de Balinski-Young, Sería deseable utilizar herramientas informáticas (por ejemplo Sage) para realizar simulaciones que ayuden a cuantificar los diversos fenómenos más o menos paradójicos que aparecen.

Bibliografía/referencias:

- M. L. Balinski, M. L, H. P. Young., The quota method of apportionment. *Amer. Math. Monthly* **82** (1975), no. 7, 701-730.
- S. J. Brams, *Mathematics and democracy designing better voting and fair-division procedures.* Princeton University Press, 2008.
- C. L Dodgson, The Principles of Parliamentary Election, Harrison $ Sons, 1884 (https://en.wikisource.org/wiki/The_Principles_of_Parliamentary_Representation)
- S. Garfunkel, *Las matemáticas en la vida cotidiana.* Addison-Wesley-Universidad Autónoma de Madrid, 1999
- J. K.Hodge, *The mathematics of voting and elections: a hands-on approach*. American Mathematical Society, 2005-