El Teorema Fundamental del Álgebra

(TFG propuesto por A. Quirós)

Que cualquier polinomio con coeficientes complejos tiene una raíz, o, en términos de álgebra abstracta, que los números complejos son un cuerpo algebraicamente cerrado, es un resultado tan importante que ha llegado a conocerse como "el Teorema Fundamental del Álgebra". Siendo fundamental, no puede sorprender que haya numerosas demostraciones del teorema, que utilizan diversas técnicas.

El objetivo del trabajo es presentar y comprender varias de ellas, desde la original de Gauss (que él mismo dijo que no era en realidad la primera), en términos de polinomios reales, a las que usan topología, geometría, variable compleja (de éstas hay varias), multiplicadores de Lagrange, teoría de Galois (y cálculo de Bachillerato: no podemos evitar completamente el análisis),.... Es interesante que nada menos que Leibniz "demostró" que el teorema era falso (el trabajo podría incorporar algunas referencias históricas)

Las demostraciones concretas que se incluyan finalmente en el trabajo dependerán de los intereses de quien lo escriba.

Bibliografía (algunas demostraciones):

- Historia del Teorema Fundamental del Álgebra en http://www-history.mcs.st-and.ac.uk/HistTopics/Fund_theorem_of_algebra.html
- R. P. Boas, Jr. A Proof of the Fundamental Theorem of Algebra. *The American Mathematical Monthly*. Vol. 42, No. 8 (Oct., 1935), pp. 501-502
- R. P. Boas, Jr.Yet Another Proof of the Fundamental Theorem of Algebra. *The American Mathematical Monthly*, Vol. 71, No. 2 (Feb., 1964), p. 180
- T. de Jong. Lagrange Multipliers and the Fundamental Theorem of Algebra. *The American Mathematical Monthly*, Vol. 116, No. 9 (Nov., 2009), pp. 828-830
- B. Fine, G. Rosenberger. *The Fundamental Theorem of Algebra*. Undergraduate Texts in Mathematics. Springer-Verlag New York, 1997.
- O. Rio Branco de Oliveira. The Fundamental Theorem of Algebra: An Elementary and Direct Proof. *The Mathematical Intelligencer*. July 2011, Volume 33, Issue 2, pp 1–2
- A. Sen. Fundamental Theorem of Algebra -- Yet Another Proof. *The American Mathematical Monthly*, Vol. 107, No. 9 (Nov., 2000), pp. 842-843

Curvas elípticas sobre cuerpos finitos

(TFG propuesto por A. Quirós)

Podemos pensar en una curva elíptica (sobre un cuerpo) como las soluciones de una ecuación polinómica de grado 3 en 2 variables (con ciertas propiedades). Una observación esencial es que los puntos de una curva elíptica forman un grupo abeliano, con una operación que se puede definir geométricamente. Si la ecuación tiene coeficientes enteros y consideramos sus soluciones módulo un primo p, estaremos ante una curva elíptica sobre el cuerpo con p elementos $\mathbb{F}_p$, y esto se puede extender a cualquier cuerpo finito. Sorprendentemente, además de su interés intrínseco, todo esto tiene notables aplicaciones tanto en matemática pura (demostración del Último Teorema de Fermat, conjetura de Birch y Swinnerton-Dyer) como aplicada (tests de primalidad, factorización, criptografía).

El objetivo del trabajo propuesto es entender el grupo de puntos de las curvas elípticas sobre cuerpos finitos, empezando por el Teorema de Hasse, que nos da una estimación del orden de este grupo (y nos permitirá una pequeña incursión en las Conjeturas de Weil). Para estudiar la estructura de este grupo conviene hacer geometría y verla sobre el cierre algebraico del cuerpo base, lo que nos llevará a estudiar el fenómeno de supersingularidad.

Dependiendo de los intereses del autor del TFG se pueden incluir también aplicaciones a la criptografía y/o desarrollar algoritmos (en SAGE o en otro lenguaje) para operar en curvas elípticas.

Bibliografía básica:

- René Schoof. Elliptic Curves. Notas de un curso en la 2008 Barbados Workshop on Computational Complexity March. Disponibles en http://cs.mcgill.ca/~denis/notes_08.pdf
- J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Springer, 2009.
- J. H. Silverman, J. Tate, *Rational points on elliptic curves***,** Springer, 1992.

Matemáticas y (diversas) elecciones
[podrían ser dos trabajos]
(TFG propuesto por A. Quirós)

El eslogan (no electoral pero sí propagandístico) con el que se podría anunciar este trabajo sería "¿cómo nos pueden ayudar las matemáticas a traducir las preferencias individuales a preferencias colectivas?". El verbo ayudar no es inocente: las matemáticas demuestran que el problema, tal y como lo hemos propuesto, no tiene una solución realmente satisfactoria (Teorema de Arrow), y que tampoco podemos delegar la decisión en un parlamento que represente proporcionalmente a la población (Teorema de Balinski-Young), pero también nos dan herramientas para analizar dónde están las dificultades y cuáles son los méritos y defectos de cada procedimiento.

El trabajo trataría de estudiar y entender desde un punto de vista matemático os métodos de toma de decisión colectiva y/o los métodos de reparto. Podría ser uno o dos trabajos (uno sobre cada uno de los dos aspectos).

Bibliografía básica:

- 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.
- S. Garfunke, J. L. Doran (trad.), E. Hernández (trad.). 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-
- E. A. Robinson. *A mathematical look at politics*. CRC Press, 2011.
- D. Saari. *Chaotic elections!: a mathematician looks at voting*. American Mathematical Society, 2001