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

Cuerpos de números algebraicos

(TFG propuesto por A. Quirós)

Un cuerpo de números algebraicos no es otra cosa que una extensión finita del cuerpo de los números racionales. Su estudio surge de manera natural al tratar problemas aritméticos, como puede ser la resolución de ecuaciones diofánticas: incluso si estamos interesaos sólo en soluciones enteras o racionales, ayuda mucho considerar cómo se comportan las ecuaciones en cuerpos de números o en sus anillos de enteros.

Pongamos dos ejemplos concretos. Cuándo se puede o no escribir un entero como suma de dos cuadrados está íntimamente ligado con la factorización en los enteros de Gauss, que no son sino el anillo de enteros del cuerpo cuadrático $\mathbb{Q}(i)$. Por otra parte, la resolución (y la no resolución) de la Ecuación de Fermat se relaciona de manera natural con los cuerpos ciclotómicos, en los que aparecen las raíces (no triviales) de la unidad.

El objetivo básico del TFG será entender la teoría de factorización de ideales en los anillos de enteros de cuerpos de números. Los principales resultados serán la factorización única de cualquier ideal como producto de ideales primos, la finitud del grupo de clases de ideales (cuyo tamaño "mide" cómo de lejos está el anillo de ser un DFU) y el Teorema de las Unidades de Dirichlet. Como aplicación, se verá la relación entre la factorización en cuerpos ciclotómicos y el Último Teorema de Fermat.

Bibliografía básica:

- O. Bordellès. Arithmetic Tales. Springer, 2012. (Capítulo 7).
- I. Stewart. Algebraic Number Theory and Fermat's Last Theorem. A.K.Peter, 2002.
- I. Stewart, D. Tall. Algebraic Number Theory (2nd ed). Chapman and Hall, 1987.
- D. Marcus. Number Fields. Springer, 1987

Curvas elípticas y criptografía

(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) y estudiar algunas de sus aplicaciones a la criptografía: criptosistemas y firmas digitales basados en el problema del logaritmo discreto para curvas elípticas, test de primalidad de Atkin-Goldwasser-Kilian y método de factorización de Lenstra.

El capítulo VI del libro de Koblitz puede servir como guión para el trabajo.

Dependiendo de los intereses de quien lo realice, el TFG puede incluir también el desarrollo, en SAGE o en otro lenguaje, de los correspondientes algoritmos.

Bibliografía básica:

- H. Cohen. A course in Computational algebraic number theory, Springer, 1993.
- H. Cohen, G. Frey. Handbook of elliptic and hyperelliptic curve cryptography, CRC, 2006.
- N. Koblitz. A course in number theory and cryptography (2nd ed.), Springer, 1994.
- R. Schoof. Elliptic Curves. Notas de un curso en la 2008 Barbados Workshop on Computational Complexity (disponibles en http://cs.mcgill.ca/~denis/notes_08.pdf)
- J. H. Silverman, The arithmet*ic of elliptic curves*, 2nd ed., Springer, 2009.
- L. Washington. Elliptic Curves: Number Theory and Cryptography (2nd ed.), CRC, 2008.

Un ejemplo de criptografía poscuántica: la criptografía basada en códigos:
(TFG propuesto por A. Quirós)

En 1994 Peter Shor propuso un algoritmo cuántico que permitiría factorizar rápidamente. Como corolario, el algoritmo permite también resolver el problema del logaritmo discreto. Por tanto, tan pronto como se desarrolle un ordenador cuántico de suficiente potencia deberemos abandonar los actuales criptosistemas de clave pública (RSA o El Gamal).

Es por tanto importante (y la Unión Europea lo ha reconocido financiando un proyecto a este respecto: https://pqcrypto.eu.org/index.html) estudiar a fondo criptosistemas de clave pública cuya seguridad no dependa de problemas que podrá resolver un ordenador poscuántico. 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 y, en particular, el que propuso Robert McEliece en 1978. Su idea no fue muy popular hasta que surgió la necesidad de resistir los ataques de los ordenadores cuánticos.

Las dos charlas de Tanja Lange recogidas en la bibliografía pueden servir como guión para el trabajo.

Dependiendo de los intereses de quien lo realice, el TFG puede incluir también el desarrollo, en SAGE o en otro lenguaje, de los correspondientes algoritmos.

Bibliografía básica:

- S. Au, C. Eubanks-Turner, J. Everson. The McEliece Cryptosystem. Manuscrito no publicado, 2013 (disponible en 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 (disponible en https://pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/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 (presentación disponible en https://www.hyperelliptic.org/tanja/vortraege/murcia.ps)
- T. Lange (con D. Bernstein). Post-quantum cryptography, Charla en la 8th Winter School on Quantum Cybersecurity, 2016 (presentación disponible en https://pqcrypto.eu.org/slides/20160117-pqc.pdf)