Propuesta de Trabajos Fin de Grado, curso académico 2018-19

PROFESOR: **Adolfo Quirós Gracián**

1.- **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

2.- **TÍTULO**: Los números p-ádicos

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. Estudiar algunas de ellas es el objetivo de este trabajo.

Bibliografía/referencias:

- 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.

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 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 el autor estuviese interesado, 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.
- J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves* (2nd ed.), Springer, 2005.

4.- **TÍTULO**: La criba en cuerpos de números

Resumen/contenido: La Criba General en Cuerpos de Números (GNFS) es el algoritmo más rápido que se conoce para factorizar números arbitrarios de más de 100 dígitos. Hay una versión "especial" muy útil para determinados números y tiene su origen en las ideas de Fermat y Kraitchick y en la Criba Cuadrática, que es su versión sobre los racionales. En el trabajo se estudiará lo suficiente sobre cuerpos de números y algoritmos de factorización como para llegar a entender la GNFS. Si el autor estuviese interesado, se podría 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.
- A. K. Lenstra and H. W. Lenstra, Jr. (eds.). *The development of the number field sieve*. Lecture Notes in Math. 1554. Springer, 1993.
- C. Pomerance. A Tale of Two Sieves. *Notices of the AMS* Vol. 43, No. 12 (Dic. 1996), 1473-1485.

5.- **TÍTULO**: Un ejemplo de criptografía poscuántica: la criptografía basada en códigos.

Resumen/contenido: 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.

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_downloaddocumen 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)