

Referencias y lecturas recomendadas

- [1] Alexandroff, P. S. *Introducción a la teoría de los grupos*. Editorial Universitaria de Buenos Aires (EUDEBA) . 151 p., (1971).
- [2] Aceña, Andrés; Armijos, Jairo; Llerena, Mario *Manual de Cálculo científico en SageMath*. [enlace](#) Observatorio Astronómico de Quito-Escuela Politécnica Nacional. 65 p., (2016) .
- [3] Baldor, J. A. *Álgebra*. Baldor Publicaciones Cultural. 876 p., (1999).
- [4] Bard, Gregory. *Sage para Estudiantes de Pregrado* . [enlace](#) (2020) .
- [5] Beezer, Robert A. *Sage Thematic Tutorials v8.9* . [enlace](#) (2005-2019).
- [6] Bourbaki, N. *Elementos De Historia De Las Matemáticas*. Alianza Editorial. 401 p., (1976).
- [7] Buchanan, William J. *Sage and ECDSA (secp256k1)* . [asecuritysite.com2024](#)
- [8] Cano P., Juan. *Algunas variantes del algoritmo cuántico de Shor*. Tesis de Grado , Facultad de Matemáticas e Informática. Universidad de Barcelona. Publicado: 13-Jun-2022
- [9] Chemla, K. *The History Of Mathematical Proof In Ancient Traditions*. Cambridge University Press . 600 p., (2012).
- [10] Contreras, R. *El Problema de los Números Congruentes*. [enlace](#),

- (2019).
- [11] Contreras, R. *Comunicación personal con Prof. Eduardo Maldonad (Dpto. física UDO)*. Julio, (2018).
 - [12] Contreras, R. *La raíz cuadrada de dos —sumerios, babilonios y griegos*. figshare.com, DOI:10.6084/m9.figshare.9943112.v1 , (2016)
 - [13] Contreras, R. *Cuaderno de notas del autor*. Centauri Tech Corp. / Universidad de los Andes. (2001).
 - [14] Descartes, R. *El discurso del método*. El CID Editor S.A.. 138 p., (1978).
 - [15] Duncan J.;Ono, K. *The math of doughnuts: 'Moonshine' sheds light on elliptic curves*. EurekAlert! , Emory Health Sciences. Publicado: 22-SEP-2017
 - [16] Goldstein, C. *El nacimiento del número* . Mundo Científico, no. 54, 11–13, (1982).
 - [17] Harvey, C *Advanced Number Theory*. Dover Publications, Inc.. 283 p., (1962).
 - [18] Houzel, C. *¿Qué es un número?*. Mundo Científico, no. 54, 6–10, (1982).
 - [19] Ifrah,G. *The Universal History Of Numbers - From Prehistory To The Invention Of The Computer*.John Wiley & Sons enlace. 656 p., (2000).
 - [20] Irby-massie, g. *Diophantus of Alexandria*. In *Dictionary of African Biography*.(Consultado el 27 Oct. 2019). oxfordreference.com 2012
 - [21] Johnson, D., Menezes, A. & Vanstone, S. *The Elliptic Curve Digital Signature Algorithm (ECDSA)*. springer.com, IJIS 1, 36–63 2001
 - [22] Judson, T.W., (Beezer, R.A.; Sage Mat.), (Behn, A.; trad.) *Algebra Abstracta Teoría y Aplicaciones*. Traducción, (2017).
 - [23] Kontorovich, A. *The Biggest Project in Modern Mathematics* YouTube, Rutgers University mathematician. 1 jun 2022. Un viaje por las matemáticas para aprender sobre las impresionantes simetrías en el corazón del programa Langlands, ilustras las formas

modulares y sus enlaces con la curvas elípticas, incluyendo cómo Andrew Wiles resolvió el último teorema de Fermat.

- [24] Mike, Mates *El Problema del Milenio sobre Curvas Elípticas* YouTube. 9 feb 2022. Explora los conceptos básicos de las curvas elípticas, aborda un problema del milenio asociado a ellas y destaca cómo conectan con áreas aparentemente no relacionadas en las matemáticas.
- [25] Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* . Bitcoin.org, bitcoin.org
- [26] National Institute of Standards and Technology (NIST). *Digital Signature Standard (DSS)*. DOI, *Federal Information Processing Standard (FIPS) 186-5* . Febrero 3, 2023. DOI: <https://doi.org/10.6028/NIST.FIPS.186-5>. CSRCURL.
- [27] NEM Group Ltd 2020. *NEM Technical Reference, version 1.2.1*. nemplatform.com , 23-02-2018
- [28] Silverman, Joseph H. *An Introduction to the Theory of Elliptic Curves*. University of Wyoming. (2006).
- [29] Sancho de Salas, Pedro José. *Algebra I. Grado en Matemáticas*. dehesa.unex.es, Universidad de Extremadura, Servicio de Publicaciones, DOI:<http://hdl.handle.net/10662/4709>, (2014)
- [30] Song, J. *Programming Bitcoin* . O'Reilly Media, Inc., (2019).
- [31] Tannery, P. *Diophanti Alexandrini opera omnia* . Leipzig. **2**, (1893–1895).
- [32] Smart, Nigel P. *How Number Theory Enables a Secure Internet*. enlace , London Mathematical Society Impact150 Stories. Publicado: 2016
- [33] Certicom Research *Standards for Efficient Cryptography / SEC 1: Elliptic Curve Cryptography*. SEC1, Certicom Corp.. Septiembre 20, 2000
- [34] Certicom Research *Standards for Efficient Cryptography / SEC 2: Recommended Elliptic Curve Domain Parameters*. SEC2, Certicom Corp.. Enero 27, 2010
- [35] Voltaire *El Siglo De Luis XIV*. Orbis.(s/f).
- [36] Wiles, Andrew; Taylor, Richard. *Modular elliptic curves and*

- Fermat last theorem*. Annals of Mathematics 3 443-551., (1995).
- [37] Wiles, Alfred *Andrew Wiles lectured on his current work around Elliptic Curves*. Oxford Mathematics London Public Lecture. (2017).
 - [38] Wiles, A. *Modular elliptic curves and Fermat's last theorem*. Ann. Math, **141**no. 3, 443–551, (1995).
 - [39] Wikipedia *René Descartes*. (2021, 24 de marzo). Wikipedia, La enciclopedia libre. Wikipedia, Consultado: 31-10-2019
 - [40] Wikipedia *"Évariste Galois"*.(2019, 24 de marzo). Wikipedia, La enciclopedia libre". Wikipedia, Consultado: 31-10-2019
 - [41] Wikipedia *"Intercambio de claves de Diffie-Hellman"*. Wikipedia, La enciclopedia libre". Wikipedia, Consultado: 25-1-2025
 - [42] Wikipedia *"Guiseeppe Peano"*.(2019, 11 de marzo). Wikipedia, La enciclopedia libre". Wikipedia, Consultado: 31-10-2019
 - [43] Wood, A. *Premio Nobel de Economía dice que cripto es lo último de una serie de monedas alternativas*. es.cointelegraph.com