El problema del logaritmo discreto: ayer, hoy y mañana

Nicolas Thériault*
Departamento de Matemática
Universidad del Bío-Bío
Concepción, Chile
ntheriau@ubiobio.cl.

Resumen

En un grupo $(G, *)$, con generador g de orden n, el problema del logaritmo discreto consiste en determinar, para cualquier elemento $h \in < g >$, cual valor de $\lambda \in \mathbb{Z}/n\mathbb{Z}$ satisface

$$[\lambda]g = g * g * g * \cdots * g = h$$
(λ veces)

Desde la introducción de la criptografía a clave publica por Diffie y Hellman en 1976 [2], el problema del logaritmo discreto se convertió en uno de las herramientas más importante para las telecomunicaciones y el comercio, aun más con la introducción de la curvas elípticas [5, 3] e hiperelípticas [4] como fuente de grupos al final de los años 1980.

En esta charla, presentaremos algunos resultados teóricos sobre el problema del logaritmo discreto en grupos "genericos" [8, 7, 6] y el efecto de estos resultados sobre la complejidad del logaritmo discreto.

En particular, veremos como la dificultad del logaritmo discrete depende del grupo en lo cual se considera, de tal forma que puede ser "sencillo" en algunos grupos, difíciles pero calculable en otros, y prácticamente intractable en otros [1], lo que tiene impacto en otros problemas, como la factorización de enteros

Finalmente, presentaremos los principales resultados de los últimos años sobre el problema del logaritmo discreto en curvas algebraicas, algunos de los resultados más recientes y de las vías más probables de desarrollo futuro.

*El trabajo es financiado por el Proyecto FONDECYT regular 1151326.

Referencias

[1] H. Cohen and G. Frey (editors). *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* Chapman & Hall / CRC, 2006.

[2] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, 22(6): 644–654, 1976.

[3] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.

[4] N. Koblitz Hyperelliptic cryptosystems. *Journal of Cryptology*, 1(3):139–150, 1989.

[5] V. Miller. Use of elliptic curves in cryptography. In *Advances in cryptology – CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer-Verlag, 1986.

[6] S.C. Pohlig and M.E. Hellman. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Transactions on Information Theory*, 24:106–110, 1978.

[7] J.M. Pollard. Monte Carlo methods for index computation (mod p). *Mathematics of Computation*, 32(143):918–924, 1978.

[8] D. Shanks. Class number, a theory of factorization and genera. In *Proc. Symp. Pure Math.*, volume 20, pages 415–440, 1971.