Blackburn, Simon R.; **Teske, Edlyn**

Baby-step giant-step algorithms for non-uniform distributions. (English) Zbl 0999.11076

Bosma, Wieb (ed.), Algorithmic number theory. 4th international symposium. ANTS-IV, Leiden, the Netherlands, July 2-7, 2000. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 1838, 153-168 (2000).

Shank's baby-step giant-step algorithm is the textbook example of a discrete-logarithm computation. It trades space for speed. (Better algorithms have been proposed by *J. M. Pollard* [Math. Comput. 32, 918-924 (1978; Zbl 0382.10001)], *S. C. Pohlig* and *M. E. Hellman* [IEEE Trans. Inf. Theory IT-24, 106-110 (1978; Zbl 0375.68023)] and *L. Adleman* [A subexponential algorithm for the discrete logarithm problem with applications to cryptography. 20th IEEE Symp. Found. Comp. Sci., 55-60 (1979)].)

The authors study a variant of this algorithm that performs extra baby steps after each giant step. With this the average run time decreases by 6, the cost of a worse worst case. The modified algorithm also performs better in the case of a non-uniform distribution of indices.

The paper gives experimental results of a large number of simulations.

For the entire collection see [Zbl 0960.00039].

Reviewer: Alexander Hulpke (Fort Collins)

MSC:

11Y16 Number-theoretic algorithms; complexity

Keywords:

automorphism group; computation