On the Cipolla-Lehmer Type Algorithms in Finite Fields

Namhun Koo[1], Gook Hwa Cho[2], Byeonghwan Go[3], Chang Heon Kim[1], and Soonhak Kwon[1]

1) *Applied Algebra and Optimization Research Center, Sungkyunkwan University, Suwon 16419, Republic of Korea*
2) *Institute for Mathematical Sciences*, *Ewha Womans University*, *Seoul 03765, Republic of Korea*
3) *Department of Mathematics, Sungkyunkwan University, Suwon 16419, Republic of Korea*

Corresponding Author: Namhun Koo, komaton@skku.edu

ABSTRACT

In this talk, we present a refinement of the Cipolla-Lehmer type algorithm[1,2] given by H. C. Williams in 1972[3], and later improved by K. S. Williams and K. Hardy in 1993[4]. For a given r-th power residue $c \in F_q$ where r is an odd prime, the algorithm of H. C. Williams determines a solution of $X^r = c$ in $O(r^3 \log q)$ multiplications in F_q, and the algorithm of K. S. Williams and K. Hardy finds a solution in $O(r^4 + r^2 \log q)$ multiplications in F_q. Our refinement finds a solution in $O(r^3 + r^2 \log q)$ multiplications in F_q. Therefore our new method is better than the previously proposed algorithms independent of the size of r, and the implementation result via SageMath shows a substantial speed-up compared with the existing algorithms. It should be mentioned that our method also works for a composite r.

REFERENCES

1. Cipolla, M., "Un metodo per la resoluzione della congruenza di secondo grado", *Rediconto dell'Accademia Scienze Fisiche e Matematiche*, Napoli, Ser. 3, Vol. IX, 1903, pp. 154-163.
2. Lehmer, D. H. "Computer technology applied to the theory of numbers", Studies in Number Theory, Englewood Cliffs, NJ: Pretice-Hall, 1969, pp.117-151.
3. Williams, H. C. "Some algorithms for solving $x^q \equiv N \pmod{p}$", *Proc. 3rd Southeastern Conf. on Combinatorics, Graph Theory, and Computing* (Florida Atlantic University), 1972, pp. 451-462.
4. Williams, K.S. and Hardy, K., "A refinement of H. C. Williams' qth root algorithm", *Mathematics of Computation*, Vol. 61, 1993, pp. 475-483.