New Cube Root Algorithm Based on Third Order Linear Recurrence Relation in Finite Field

Gook Hwa Cho, Namhun Koo, Eunhye Ha, and Soonhak Kwon

Email: achimheasal@nate.com, komaton@skku.edu, grace.eh.ha@gmail.com, shkwon@skku.edu

Dept. of Mathematics, Sungkyunkwan University, Suwon, S. Korea

Abstract

We present a new cube root algorithm in finite field $\mathbb{F}_q$ with q a power of prime, which extends Cipolla-Lehmer type algorithms and has lower complexity than Tonelli-Shanks type algorithms.

Efficient computation of r-th root in $\mathbb{F}_q$ has many applications in computational number theory and many other related areas. There are two standard algorithms for computing r-th root in finite field. One is Adleman-Manders-Miller algorithm which is a straightforward generalization of Tonelli-Shanks square root algorithm.

Another algorithm is a also a natural generalization of Cipolla-Lehmer square root algorithm. Original Cipolla-Lehmer algorithm requires one to use extension field arithmetic in $\mathbb{F}_{q^2}$, but one can use second order linear recurrence relation without any extension field arithmetic. Moreover a special type of Lucas sequence method of Müller gives a new square root algorithm which is consistently better than Tonelli-Shanks.

However unlike the cases of Tonell-Shanks and Cipolla-Lehmer, extending the idea of Müller to cube root algorithm is not so obvious because, for given cubic residue $c \in \mathbb{F}_q$, one needs to find a cubic polynomial $f(x)$ with nice coefficients (i.e., with norm of f equal to one) and a suitable m such that $Tr(\alpha^m) = \alpha^m + \alpha^{mq} + \alpha^{mq^2}$ with $f(\alpha) = 0$ is a cube root of c.

In this paper, we show that the above question can be answered affirmatively. That is, for given cubic residue $c \in \mathbb{F}_q$ with $q \equiv 1 \pmod 9$, we find an irreducible polynomial $f(x) = x^3 - ax^2 + bx - 1$ with root $\alpha \in \mathbb{F}_{q^3}$ such that $Tr(\alpha^{\frac{q^2+q-2}{9}})$ is a cube root of c. Consequently we find an efficient cube root algorithm which can be easily computed via simple third order linear recurrence sequence arising from $f(x)$. Since it is easy to find closed formulas for cube root when $q \equiv 4, 7 \pmod 9$ or when $q \equiv 2 \pmod 3$, our cube root algorithm is applicable for any prime power q. Complexity estimation shows that our algorithm is consistently better than previously proposed Tonelli-Shanks and Cipolla-Lehmer type algorithms.

Keywords : finite field, cube root, linear recurrence relation, Tonell-Shanks algorithm, Cipolla-Lehmer algorithm, Adleman-Manders-Miller algorithm

References

[1] S. Müller, *On the computation of square roots in finite fields*, Design, Codes and Cryptography, Vol.31, pp. 301-312, 2004