Remarks on the Pocklington and Padró-Sáez Cube Root Algorithm in $\mathbb{F}_q$

Geon Heo[†], Seokhwan Choi[†], Kwang Ho Lee[†], Namhun Koo[‡] and Soonhak Kwon[‡]
Gyeonggi Science High School for the Gifted, Suwon, S. Korea[†]
Dept. of Mathematics, Sungkyunkwan University, Suwon, S. Korea[‡]
shkwon@skku.edu

Abstract

We clarify and generalize a cube root algorithm in $\mathbb{F}_q$ proposed by Pocklington [1], and later rediscovered by Padró and Sáez [2]. We correct some mistakes in [2] and give a full generalization of the result in [1, 2] for the cube root algorithm. We also give the comparison of the implementation of Pocklington and Padró-Sáez algorithm with two most popular cube root algorithms, namely the Adleman-Manders-Miller algorithm and the Cipolla-Lehmer algorithm. To the authors' knowledge, our comparison is the first one which compares three basic algorithms together.

Keywords : cube root algorithm, finite field, Pocklington algorithm, Adleman-Manders-Miller algorithm, Cipolla-Lehmer algorithm

1 Introduction

Pocklington [1] proposed a new square and cube root algorithms in the finite field $\mathbb{F}_q$ with q a prime, which are different from the two most well-known algorithms nowadays; the Adleman-Manders-Miller algorithm [4, 5, 6, 7] and the Cipolla-Lehmer [8, 9, 10, 11] algorithm. Later, the algorithm of Pocklington is rediscovered by Peralta [3] for the case of the square root and by Padró and Sáez [2] for the case of the cube root.

Both Peralta and Padró-Sáez were unaware of the work of Pocklington at the time of their results (See also [12]). Padró and Sáez, knowing the result of Peralta [3], gave a cubic version of the Peralta square root algorithm, and their algorithm has a more general form (with the estimation of the success probability) than the original version of Pocklington. However it contains some flaws (in Proposition 3.5 of [2]) where some cases which cannot happen are considered. Moreover, no available literature including the review of the paper [2] in MathSciNet [13] notices this error.

Our aim in this paper is to correct the errors in the result of Padró-Sáez [2] and to present a refinement of the cube root algorithm extending both the result of Pocklington and Padró-Sáez. We also give the result of the software implementations (using SAGE) of the Pocklington and Padró-Sáez algorithm and two other standard algorithms; the Adleman-Manders-Miller algorithm and the Cipolla-Lehmer algorithm. To the authors' knowledge, our comparison is the first one ever which compares all three algorithms together. Our result shows that the Pocklington and Padró-Sáez algorithm is consistently superior to the Cipolla-Lehmer algorithm, and is also superior to the Adleman-manders-Miller algorithm when s is large, where s is the largest integer satisfying $3^s|q-1$.

2 Pocklington and Padró-Sáez Cube Root Method

Both Pocklington [1] and Padró-Sáez [2] considered the finite field $\mathbb{F}_q$ with prime q. However their approaches are also good for the general finite field. Therefore we assume that q is a power of a prime and let $\mathbb{F}_q$ be a finite field with q elements. Let $a \neq 0 \in \mathbb{F}_q$ be a cubic residue in $\mathbb{F}_q$, i.e., there exists $x \in \mathbb{F}_q$ such that $x^3 = a$.

Note that when $q \equiv 2 \pmod 3$, a cube root of a is given as $a^{\frac{2q-1}{3}}$, and when $q \equiv 0 \pmod 3$ (i.e., when $q = 3^s$), then a cube root of $a \in \mathbb{F}_{3^s}$ is given as $a^{3^{s-1}}$. Therefore a cube root of a can be found easily when $q \equiv 0, 2 \pmod 3$. When $q \equiv 1 \pmod 3$, there exists a primitive cube root of unity $\epsilon \in \mathbb{F}_q$ satisfying $\epsilon^3 = 1$. From now on, we will only consider the finite field $\mathbb{F}_q$ with $q \equiv 1 \pmod 3$, and a primitive cube root of unity ϵ is fixed throughout this paper.

For a given cube root $x \in \mathbb{F}_q$ of a, the other two cube roots of a are given as ϵx and $\epsilon^2 x$, and we have the polynomial identity

$$X^3 - a = (X - x)(X - \epsilon x)(X - \epsilon^2 x) \in \mathbb{F}_q[X].$$

We also have the following isomorphism of rings

$$\mathbb{F}_q[X]/\langle X^3 - a\rangle \cong \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q, \tag{1}$$

where the isomorphism is given as

$$\begin{aligned} \varphi : \mathbb{F}_q[X]/\langle X^3 - a\rangle &\longrightarrow \qquad\qquad \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \\ \alpha + \beta X + \gamma X^2 &\mapsto (\alpha + \beta x + \gamma x^2, \alpha + \beta\epsilon x + \gamma\epsilon^2 x^2, \alpha + \beta\epsilon^2 x + \gamma\epsilon x^2) \end{aligned} \tag{2}$$

For a detailed explanation, see [2]. We also need the norm of $z = \alpha + \beta X + \gamma X^2 \in \mathbb{F}_q[X]/\langle X^3 - a\rangle$, $N(z)$, defined as the product of all the conjugates of z,

$$N(z) = z\bar{z}\bar{\bar{z}} \in \mathbb{F}_q,$$

where $\bar{z} = \alpha + \beta\epsilon X + \gamma\epsilon^2 X^2$. Then the following is well-known;

$$\begin{aligned} N(z) &= (\alpha + \beta X + \gamma X^2)(\alpha + \beta\epsilon X + \gamma\epsilon^2 X^2)(\alpha + \beta\epsilon^2 X + \gamma\epsilon X^2) \\ &= (\alpha + \beta x + \gamma x^2)(\alpha + \beta\epsilon x + \gamma\epsilon^2 x^2)(\alpha + \beta\epsilon^2 x + \gamma\epsilon x^2) \end{aligned} \tag{3}$$

Define the set of invertible elements as $\mathbb{F}_q^\times$ and $(\mathbb{F}_q[X]/\langle X^3 - a\rangle)^\times$. Then from the equations (2) and (3), we have

$$N(z) \neq 0 \Longleftrightarrow \varphi(z) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times \times \mathbb{F}_q^\times,$$

which implies that we also have the isomorphism between the sets of invertible elements;

$$(\mathbb{F}_q[X]/\langle X^3 - a\rangle)^\times \cong \mathbb{F}_q^\times \times \mathbb{F}_q^\times \times \mathbb{F}_q^\times \tag{4}$$

For a given $z = \alpha + \beta X + \gamma X^2 \in \mathbb{F}_q[X]/\langle X^3 - a\rangle$, the norm of z is the determinant of the linear transformation $\ell_z : \mathbb{F}_q[X]/\langle X^3 - a\rangle \longrightarrow \mathbb{F}_q[X]/\langle X^3 - a\rangle$ with $\ell_z(w) = wz$, and it can be computed as follows.

Lemma 1. *One has*

$$N(z) = \begin{vmatrix} \alpha & \beta & \gamma \\ a\gamma & \alpha & \beta \\ a\beta & a\gamma & \alpha \end{vmatrix} = \alpha^3 + a\beta^3 + a^2\gamma^3 - 3a\alpha\beta\gamma. \tag{5}$$

Proof. By expanding the product in the equation (3), and using the properties $x^3 = a$ and $1 + \epsilon + \epsilon^2 = 0$, one gets the right side of the equation (5), which can also be written as a determinant form. $\square$

Note that the cost of computing $N(z)$ is 11 multiplications in $\mathbb{F}_q$ and is negligible compared with the cost of the exponentiation z^t when t is large.

Now we are ready to present the original version of the Proposition given in [2].

Proposition 1 (Proposition 3.5 in [2])**.** *Let $a \neq 0 \in \mathbb{F}_q$ be a cubic residue and $z = \alpha+\beta X+\gamma X^2$ be an element of $\mathbb{F}_q[X]/\langle X^3 - a\rangle$ where at least two of the coefficients α, β and γ are nonzero. Then*

(1) *If $z^3 = \alpha'$ with $\alpha' \in \mathbb{F}_q^\times$, then*

- (1a) *if β and γ are nonzero, then $\sqrt[3]{a} = \frac{\alpha}{\beta}$,*
- (1b) *if $\beta = 0$ and α, γ are nonzero, then $\sqrt[3]{a} = \frac{1}{a}(\frac{\alpha}{\gamma})^2$,*
- (1c) *if $\gamma = 0$ and α, β are nonzero, then $\sqrt[3]{a} = -\frac{\alpha}{\beta}$,*

(2) *If $z^3 = \beta' X$ with $\beta' \in \mathbb{F}_q^\times$, then $\sqrt[3]{a} = \frac{N(z)}{\beta'}$*

(3) *If $z^3 = \gamma' X^2$ with $\gamma' \in \mathbb{F}_q^\times$, then $\sqrt[3]{a} = \frac{N(z)^2}{\gamma'^2 a}$*

3 New Refined Algorithm

As a result of the various mathematical softwares (such as MAPLE and SAGE) implementations, we found out that the cases (1b) and (1c) of Proposition 3.5 in [2] never appear in practice. We also found out that the cases (2) and (3) do happen only when $q \equiv 1 \pmod 9$. These contradicting implementation results can be explained rigorously by the following mathematical analysis.

Lemma 2. *Assuming the same conditions in Proposition 3.5 of [2],*

(1) *The cases* (1b) *and* (1c) *cannot happen. In other words, the assumption of* (1b) [$\beta = 0$ *and* α, γ *are nonzero*] *or the assumption of* (1c) [$\gamma = 0$ *and* α, β *are nonzero*] *imply $z^3 \notin \mathbb{F}_q$.*

(2) *The cases* (2) *and* (3) *do happen only when $q \equiv 1 \pmod 9$.*

Proof. (1) Our proof relies on the following identity in $\mathbb{F}_q[X]/\langle X^3 - a\rangle$,

$$\begin{aligned} z^3 &= (\alpha + \beta X + \gamma X^2)^3 \\ &= (\alpha^3 + a\beta^3 + a^2\gamma^3 + 6a\alpha\beta\gamma) + 3(\alpha\gamma^2 a + \beta^2\gamma a + \alpha^2\beta)X + 3(\alpha^2\gamma + \alpha\beta^2 + \beta\gamma^2 a)X^2. \end{aligned} \tag{6}$$

From the above identity, letting $\beta = 0$, one has

$$z^3 = (\alpha + \gamma X^2)^3 = \alpha^3 + \gamma^3 a^2 + 3\alpha\gamma^2 aX + 3\alpha^2\gamma X^2. \tag{7}$$

Therefore $\alpha \neq 0, \gamma \neq 0$ implies $z^3 \notin \mathbb{F}_q$, which contradicts the assumption of (1) of Proposition 3.5 saying $z^3 = \alpha' \in \mathbb{F}_q$. In the same way, letting $\gamma = 0$ in the equation (6), we have

$$z^3 = (\alpha + \beta X)^3 = \alpha^3 + \beta^3 a + 3\alpha^2\beta X + 3\alpha\beta^2 X^2. \tag{8}$$

Therefore $\alpha \neq 0, \beta \neq 0$ implies $z^3 \notin \mathbb{F}_q$, which also contradicts the assumption of (1) of Proposition 3.5 in [2].

(2) Now we will show that the cases (2) and (3) of Proposition 3.5 can happen only when $q \equiv 1 \pmod 9$. Since $q \equiv 1 \pmod 3$, we may write

$$q = 3(3k+m)+1 = 9k+3m+1, \quad \text{for some } k \in \mathbb{Z} \text{ and } m \in \{0,1,2\}.$$

From the isomorphism in the equation (4), we have $z^{q-1} = 1$ for all $z \in (\mathbb{F}_q[X]/\langle X^3 - a\rangle)^\times$. Therefore the case (2) $z^3 = \beta' X$ implies that

$$1 = z^{q-1} = (z^3)^{\frac{q-1}{3}} = (\beta' X)^{3k+m} = (\beta')^{3k+m} a^k X^m \in \mathbb{F}_q.$$

Consequently we get $m = 0$ and $q = 9k+1$. In the same way, the case (3) $z^3 = \gamma' X^2$ implies that

$$1 = z^{q-1} = (z^3)^{\frac{q-1}{3}} = (\gamma' X^2)^{3k+m} = (\gamma')^{3k+m} a^{2k} X^{2m} \in \mathbb{F}_q.$$

Since the possible values of X^{2m} are $1, X^2, X^4 = aX$, we also get $m = 0$ and $q = 9k+1$. □

Because of this observation, Proposition 3.5 in [2] should be modified, and the corrected and extended version is given here.

Proposition 2 (Corrected and Extended Version of Proposition 3.5 in [2])**.** *Let $a \neq 0 \in \mathbb{F}_q$ be a cubic residue and let $z = \alpha + \beta X + \gamma X^2$ be a nonzero element of $\mathbb{F}_q[X]/\langle X^3 - a\rangle$.*

(1) *If $z^3 = \alpha'$ with $\alpha' \in \mathbb{F}_q^\times$ where at least two of α, β, γ are nonzero, then all three α, β, γ are nonzero and all three distinct cube roots of a are given as $\frac{\alpha}{\beta}, \frac{\beta}{\gamma}$ and $\frac{a\gamma}{\alpha}$.*

(2) *If $z^3 = \beta' X$ or $z^3 = \gamma' X^2$ for some $\beta', \gamma' \in \mathbb{F}_q^\times$, then all three α, β, γ are nonzero and*

  (2a) *if $z^3 = \beta' X$, then $\sqrt[3]{a} = -\frac{9a\alpha\beta\gamma}{\beta'}$.*

  (2b) *if $z^3 = \gamma' X^2$, then $\sqrt[3]{a} = -\frac{\gamma'}{9\alpha\beta\gamma}$.*

Proof. (1) From the equations (7) and (8), we already showed that two nonzero coefficients α, γ with $\beta = 0$ or α, β with $\gamma = 0$ produce $z^3 \notin \mathbb{F}_q$. The remaining case where β, γ are nonzero and $\alpha = 0$ can be understood from the following identity derived from the equation (6),

$$z^3 = (\beta X + \gamma X^2)^3 = \gamma^3 a^2 + \beta^3 a + 3a\beta^2\gamma X + 3a\beta\gamma^2 X^2, \tag{9}$$

which shows $z^3 \notin \mathbb{F}_q$. Therefore, if at least two of α, β and γ are nonzero and if $z^3 \in \mathbb{F}_q$, then one must have all nonzero α, β and γ. The fact that $a = \left(\frac{\alpha}{\beta}\right)^3$ is already shown both in [1] and [2]. Since $z^3 = \alpha' \in \mathbb{F}_q$, from the equation (6), we get

$$\alpha\gamma^2 a + \beta^2\gamma a + \alpha^2\beta = 0, \tag{10}$$
$$\alpha^2\gamma + \alpha\beta^2 + \beta\gamma^2 a = 0. \tag{11}$$

Then $\gamma\times(10) - \beta\times(11) = \alpha(\gamma^3 a - \beta^3) = 0$, from which we get $a = \left(\frac{\beta}{\gamma}\right)^3$. Also $\alpha\times(10) - \gamma a\times(11) = \beta(\alpha^3 - \gamma^3 a^2) = 0$, from which we have $a = \left(\frac{\gamma a}{\alpha}\right)^3$. Also notice that $\beta\times(10) - \alpha\times(11) =$

$\gamma(\beta^3 a - \alpha^3) = 0$, which says $a = \left(\frac{\alpha}{\beta}\right)^3$. All three cube roots $\frac{\alpha}{\beta}, \frac{\beta}{\gamma}, \frac{a\gamma}{\alpha}$ are different because $\frac{\alpha}{\beta} + \frac{\beta}{\gamma} + \frac{a\gamma}{\alpha} = \frac{1}{\alpha\beta\gamma}(\alpha^2\gamma + \alpha\beta^2 + \beta\gamma^2 a) = 0$ from the equation (11).

(2) In view of Lemma 1, the constant term of the equation (6) is $N(z) + 9a\alpha\beta\gamma$. Therefore one has $N(z) = -9a\alpha\beta\gamma$ if $z^3 = \beta' X$ or $z^3 = \gamma' X^2$. For the case (2a), by taking norm to $\beta' X = z^3$, we get $\beta'^3 a = N(z)^3 = (-9a\alpha\beta\gamma)^3$ and thus $a = \left(-\frac{9a\alpha\beta\gamma}{\beta'}\right)^3$. For the case (2$b$), by taking norm to $z^3 X = \gamma' a$, we get $N(z)^3 a = \gamma'^3 a^3$ and thus $a = \left(-\frac{\gamma'}{9\alpha\beta\gamma}\right)^3$. Note that $\alpha\beta\gamma \neq 0$, because one gets $a = 0$ if $\alpha\beta\gamma = 0$. $\square$

The fact $\frac{\beta}{\gamma}$ is a root of $X^3 - a = 0$ is also noticed in [1], but the fact that $\frac{a\gamma}{\alpha}$ is the other root of $X^3 - a = 0$ different from $\frac{\alpha}{\beta}$ and $\frac{\beta}{\gamma}$ are not mentioned in both [1] and [2]. Also note that computing $a\alpha\beta\gamma$ requires 3 multiplications while computing $N(z)$ requires 11 multiplications.

Proposition 3. *Let q be a prime power with $q-1 = 3^s t$ and $\gcd(3,t) = 1$. Let $0 \leq m \leq s-1$. Then the probability that a randomly chosen invertible $z \in \mathbb{F}_q[X]/\langle X^3 - a\rangle$ satisfies $z^{3^m t} = \alpha' + \beta' X + \gamma' X^2$ with exactly 2 zero coefficients is $\frac{1}{3^{2s-2m-1}}$.*

Proof. We have to find the probability that $z^{3^m t} = \alpha'$ or $z^{3^m t} = \beta' X$ or $= \gamma' X^2$. Note that these three cases are independent cases.
Case 1. $z^{3^m t} = \alpha'$: Due to the isomorphism in the equation (4), we may assume $\varphi(z) = (a,b,c) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times \times \mathbb{F}_q^\times$ and $(\alpha', \alpha', \alpha') = \varphi(z^{3^m t}) = \varphi(z)^{3^m t} = (a^{3^m t}, b^{3^m t}, c^{3^m t})$. Thus from $a^{3^m t} = b^{3^m t} = c^{3^m t} \in \mathbb{F}_q^\times$, we get $\left(\frac{b}{a}\right)^{3^m t} = 1$ and $\left(\frac{c}{a}\right)^{3^m t} = 1$. Therefore such (a,b,c) can be parameterized as $(a,b,c) = (a, a\zeta, a\zeta')$ with $a \in \mathbb{F}_q^\times$ and $\zeta, \zeta' \in C$, where C is a unique (cyclic) subgroup of order $3^m t$ in $\mathbb{F}_q^\times$. Consequently the number of such (a,b,c) is $(q-1)3^{2m}t^2$.
Case 2. $z^{3^m t} = \beta' X$: In the same way, we may assume $\varphi(z) = (a,b,c) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times \times \mathbb{F}_q^\times$ and $(\beta' x, \beta' x\epsilon, \beta' x\epsilon^2) = \varphi(z^{3^m t}) = \varphi(z)^{3^m t} = (a^{3^m t}, b^{3^m t}, c^{3^m t})$. Thus we get $\left(\frac{b}{a}\right)^{3^m t} = \epsilon$ and $\left(\frac{c}{a}\right)^{3^m t} = \epsilon^2$. Since $m+1 \leq s$ (i.e., $3^{m+1}t | q-1 = 3^s t$), there is a primitive $3^{m+1}t$-th root of unity μ such that either $\mu^{3^m t} = \epsilon$ or ϵ^2. Therefore letting $(\theta, \theta') = (\mu, \mu^2)$ or (μ^2, μ), one has $(\theta^{3^m t}, \theta'^{3^m t}) = (\epsilon, \epsilon^2)$ which implies $\left(\frac{b}{a\theta}\right)^{3^m t} = 1$ and $\left(\frac{c}{a\theta'}\right)^{3^m t} = 1$. Similarly as in the Case 1, such a,b,c can be parimetrized as $(a,b,c) = (a, a\theta\zeta, a\theta'\zeta')$ where $a \in \mathbb{F}_q^\times$, $\zeta, \zeta' \in C$, and the number of such (a,b,c) is also $(q-1)3^{2m}t^2$.
Case 3. $z^{3^m t} = \gamma' X^2$: This case can be dealt in the same manner with the Case 2 so that the number of possible cases of z is $(q-1)3^{2m}t^2$.

Therefore the desired probability is $\frac{3 \cdot 3^{2m}t^2(q-1)}{(q-1)^3} = \frac{3 \cdot 3^{2m}t^2}{(q-1)^2} = \frac{3 \cdot 3^{2m}t^2}{3^{2s}t^2} = \frac{1}{3^{2s-2m-1}}$. $\square$

As a special case, when $m = 0$, we get the probability that $z^t = \alpha'$ or $\beta' X$ or $\gamma' X^2$ as $\frac{1}{3^{2s-1}}$, which is the result of Proposition 3.7 in [2] . Also note that this result does not contradict Lemma 2–(2), because $z^t = \beta' X, \gamma' X^2$ are possible since $3 \not| t$.

Our observations on Proposition 2 and 3 lead to a cube root algorithm shown in Algorithm 1, whose complexity is $O(\log^3 q)$ since the cost of the algorithm is several exponentiations in $\mathbb{F}_q$. In the algorithm, we try random invertible $z \in \mathbb{F}_q[X]/\langle X^3 - a\rangle$ until we find z^t with at least two nonzero coefficients. Then, we apply repeated cubings to z^t until we have $z^{3^m t} \in \mathbb{F}_q$ or $\mathbb{F}_q \cdot X$ or $\mathbb{F}_q \cdot X^2$ for some $1 \leq m \leq s$. Note that, since $z^{3^s t} = z^{q-1} = 1$ when z is invertible, such m always exists once we have z^t with at least two nonzero coefficients. Because of Proposition 3, the probability of having only one nonzero coefficient in Step 6 is $\frac{1}{3^{2s-1}}$, and the probability of finding a cube root exactly after m-th iteration of the while-loop is $\frac{1}{3^{2s-(2m+1)}} - \frac{1}{3^{2s-(2m-1)}}$

for $1 \le m \le s-1$. The probability of finding a cube root after full iterations (i.e., after s-th iteration) is $\frac{2}{3}$. Therefore the expected number of iterations of the while-loop is

$$\sum_{m=1}^{s-1} m\left(\frac{1}{3^{2s-(2m+1)}} - \frac{1}{3^{2s-(2m-1)}}\right) + s\left(1-\frac{1}{3}\right) = s - \sum_{m=1}^{s} \frac{1}{3^{2m-1}} = s - \frac{3}{8}\left(1-\frac{1}{9^s}\right).$$

Algorithm 1 Refined Pocklington and Padró-Sáez Cube Root Algorithm

---

Input : A cube a in $\mathbb{F}_q$ with $q-1 = 3^s t,\ \gcd(3,t)=1$

Output : x satisfying $x^3 = a$ in $\mathbb{F}_q$

1: **if** $q \equiv 4 \pmod 9$ **then** $x \leftarrow a^{\frac{2q+1}{9}}$
2: **if** $q \equiv 7 \pmod 9$ **then** $x \leftarrow a^{\frac{q+2}{9}}$
3: Choose random $\alpha, \beta, \gamma \in \mathbb{F}_q$ and let $z := \alpha + \beta X + \gamma X^2 \in \mathbb{F}_q[X]/\langle X^3 - a\rangle$
4: **if** $N(z) = 0$ **then** go to STEP 3
5: $z \leftarrow z^t$
6: **if** $\alpha = \beta = 0$ or $\beta = \gamma = 0$ or $\gamma = \alpha = 0$ **then** go to STEP 3
7: **while** $\alpha\beta \ne 0$ or $\beta\gamma \ne 0$ or $\gamma\alpha \ne 0$ **do** //while at least two of α, β, γ are nonzero//
8: $\quad z_0 := \alpha_0 + \beta_0 X + \gamma_0 X^2 \leftarrow z$ (i.e., $\alpha_0 \leftarrow \alpha,\ \beta_0 \leftarrow \beta,\ \gamma_0 \leftarrow \gamma$)
9: $\quad z \leftarrow z^3$
10: **if** $\beta = \gamma = 0$ **then** $x \leftarrow \frac{\alpha_0}{\beta_0}$
11: **else if** $\gamma = \alpha = 0$ **then** $x \leftarrow -\frac{9a\alpha_0\beta_0\gamma_0}{\beta}$
12: **else** **then** $x \leftarrow -\frac{\gamma}{9\alpha_0\beta_0\gamma_0}$
13: **return** x

In the given algorithm, the probability that a randomly chosen $z \in \mathbb{F}_q[X]/\langle X^3 - a\rangle$ is invertible (i.e., $N(z) \ne 0$) is $\left(1-\frac{1}{q}\right)^3$. Therefore when the finite field $\mathbb{F}_q$ is very large, one may safely assume $N(z) \ne 0$, and thus the STEP 4 in the algorithm may be omitted with error probability $1 - \left(1-\frac{1}{q}\right)^3 \approx \frac{3}{q}$. In the event of the extremely unlucky case $N(z) = 0$, omitting the STEP 4 gives endless while-loop because one has $z^{q-1} \ne 1$ if and only if $N(z) = 0$. Any way, the computational cost of the STEP 4 is just 11 multiplications in $\mathbb{F}_q$ and is negligible compared with the total cost of the algorithm. Also, the probability that one may go back to the STEP 3 in the STEP 6 is $\frac{1}{3^{2s-1}} \le \frac{1}{27}$, since one reaches the STEP 6 only if $s \ge 2$ (i.e., if $q \equiv 1 \pmod 9$).

4 Comparison Results

We compared our proposed algorithm with two most well-known cube root algorithms in the finite field $\mathbb{F}_q$; the AMM (Adleman-Manders-Miller) algorithm [4, 5, 6, 7] and the CM (Cipolla-Lehmer) algorithm [8, 9, 10, 11]. The complexity of the AMM cube root algorithm is $O(\log^3 q + s^2 \log^2 q)$ where $q-1 = 3^s t$ with $\gcd(3,t)=1$, and the complexity of the CM cube root algorithm is $O(\log^3 q)$ which is same to the Pocklington and Padró-Sáez algorithm.

We used a standard version in [7] for the AMM implementation. For the Cipolla-Lehmer implementation, we used two algorithms; the algorithm of H. C. Williams [10] and the algorithm of K. S. Williams and K. Hardy [11]. The algorithm in [10] is a generalization to the r-th root extraction (with the recurrence relation technique) of the original Cipolla-Lehmer

Table 1: Running time (in seconds) for cube root computation with $p \approx 2^{2000}$

s	50	100	150	200	250	300
AMM [6, 7]	0.082	0.148	0.297	0.498	0.781	1.084
CM [10]	0.495	0.495	0.498	0.497	0.488	0.492
CM [11]	0.282	0.284	0.284	0.285	0.276	0.282
Proposed Alg.	0.236	0.235	0.235	0.236	0.234	0.233

Table 2: Running time (in seconds) for cube root computation with $p \approx 2^{3000}$

s	50	100	150	200	250	300
AMM [6, 7]	0.150	0.292	0.519	0.842	1.294	1.746
CM [10]	1.363	1.350	1.395	1.382	1.352	1.465
CM [11]	0.756	0.744	0.790	0.778	0.750	0.796
Proposed Alg.	0.655	0.655	0.654	0.651	0.651	0.648

square root algorithm [8, 9], and the algorithm in [11], a refinement of the algorithm in [10], has a better complexity for small values of r. Tables 1 and 2 show the comparison of the implementation results with SAGE of the above mentioned 3 algorithms and our proposed one. The implementation was performed on Intel Core i7-4770 3.40GHz with 8GB memory.

For convenience, we used prime fields $\mathbb{F}_p$ with two different size of primes p: 2000 and 3000 bits. Average timings of the cube root computations for 5 different inputs of cubic rsidue $a \in \mathbb{F}_p$ are computed for those cases $s = 50, 100, 150, \cdots$, etc. As one can see in the tables, the timings of the AMM increase drastically as s becomes larger, while the timings of the CM algorithms and our algorithm are independent of s. The tables also show that our proposed algorithm is consistently faster than the Cipolla-Lehmer. For example, when $p \approx 2^{3000}$, the average timing of the Cipolla-Lehmer in [11] is 0.769 (seconds) which are 20% slower than the average timing 0.652 (seconds) of the proposed algorithm.

5 Conclusion

We corrected some errors in the Pocklington and Padró-Sáez cube root algorithm in [2], and proposed a refined algorithm. The implementation result shows that the proposed algorithm is faster than the Adleman-Manders-Miller algorithm for large values of s, and is also consistintly faster than the Cipolla-Lehmer algorithm. The difference between the Pocklington and Padró-Sáez algorithm and the Cipolla-Lehmer algorithm is that, though they have the same complexity, the Pocklington and Padró-Sáez algorithm relies on the ring arithmetic in $\mathbb{F}_q[X]/\langle X^3 - a\rangle$ which is isomorphic to $\mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q$, while the Cipolla-Lehmer algorithm relies on the arithmetic in the extension filed $\mathbb{F}_{q^3}$. Therefore, to find a cube root, essentially one only needs to compute z^{q-1} in the Pocklington and Padró-Sáez while one has to compute $z^{\frac{q^3-1}{q-1}} = z^{q^2+q+1}$ in the Cipolla-Lehmer [10, 11]. This difference of the exponents (of z) explains the superior performance of the Pocklington and Padró-Sáez over the Cipolla-Lehmer. For the quadratic case, there is no such difference, i.e., z^{q-1} in the Pocklington and Padró-Sáez versus

z^{q+1} in the Cipolla-Lehmer. We finally remark that, as far as we know, our implementation of the 3 major algorithms (the Adleman-Manders-Miller, the Cipolla-Lehmer and the Pocklington and Padró-Sáez) is the first one available in the literature.

References

[1] H. C. Pocklington, "The direct solution of the quadratic and cubic binomial congruences with prime moduli", *Proceedings of the Cambridge Philosophical Society*, vol. 19, pp. 57-59, 1917.

[2] C. Padró and G. Sáez, "Taking cube roots in $\mathbb{Z}_m$", *Applied Mathematics Letters*, vol. 15, pp. 703-708, 2002.

[3] R. C. Peralta, "A simple and fast probabilistic algorithm for computing square roots modulo a prime number", *IEEE Transactions on Information Theory*, vol. 32, pp. 846-847, 1986.

[4] D. Shanks "Five number-theoretic Algorithms," *Proceeding of Second Manitoba Conference of Numerical Mathematics*, pp.51-70, 1972.

[5] A. Tonelli, "Bemerkung über die Auflösung Quadratischer Congruenzen", *Göttinger Nachrichten*, pp.344-346, 1891.

[6] L. Adleman, K. Manders and G. Miller, "On taking roots in finite fields", *Proc. 18th IEEE Symposium on Foundations on Computer Science (FOCS)*, pp. 175-177, 1977.

[7] Z. Cao, Q. Sha, and X. Fan, "Adlemen-Manders-Miller root extraction method revisited", preprint, available at http://arxiv.org/abs/1111.4877, 2011.

[8] M. Cipolla, "Un metodo per la risolutione della congruenza di secondo grado", *Rendiconto dell'Accademia Scienze Fisiche e Matematiche*, Napoli, Ser. 3, vol. IX, pp. 154-163, 1903.

[9] D. H. Lehmer, "Computer technology applied to the theory of numbers", In *Studies in Number Theory*, Prentice-Hall Enblewood Cliffs, NJ, pp.117-151, 1969.

[10] H. C. Williams, "Some algorithm for solving $x^q \equiv N \pmod p$", *Proc. 3rd Southeastern Conf. on Combinatorics, Graph Theory, and Computing*, Florida Atlantic University, pp. 451-462, 1972.

[11] K. S. Williams and K. Hardy, "A refinement of H. C. Williams' qth root algorithm", Mathematics of Computation, Vol.61, pp. 475-483, 1993.

[12] D. Bernstein, "Faster square roots in annoying finite fields", preprint, available at http://cr.yp.to/papers/sqroot.pdf.

[13] American Mathematical Society, "MathSciNet Review", available at http://www.ams.org/mathscinet.