PERGAMON

Applied Mathematics Letters 15 (2002) 703–708

Applied Mathematics Letters

www.elsevier.com/locate/aml

Taking Cube Roots in $\mathbb{Z}_m$

C. PADRÓ AND G. SÁEZ

Dep. Matemàtica Aplicada IV, Univ. Politècnica de Catalunya

c/Jordi Girona, 1-3 (C3–202), 08034-Barcelona, Spain

<matcpl><german>@mat.upc.es

(Received August 2000; revised and accepted July 2001)

Abstract—We address the problem of taking cube roots modulo an integer. We generalize two of the fastest algorithms for computing square roots modulo a prime to algorithms for computing cube roots.

Keywords—Cube root, Peralta algorithm, Tonelli-Shanks algorithm, Cryptography.

1. INTRODUCTION

The existence and computation of square roots modulo a composite number m are behind many of the theoretical and practical problems in number theory. The problem of how to calculate square roots is computationally equivalent to the factorization of m, which is considered to be a computationally hard problem. This problem is used in some cryptosystems.

Several algorithms have been described for computing square roots modulo a prime number p, but no specific algorithms have been published for computing cube roots modulo p. The main algorithms for taking square roots are: general algorithms for factoring polynomials [1], Adleman-Manders-Miller algorithm [2], Tonelli-Shanks algorithm [3], Peralta algorithm [4], Schoof algorithm [5], and Lehmer algorithm [6].

This paper presents algorithms for taking cube roots on a field $\mathbb{Z}_p$ for large p. These algorithms can be applied to compute cube roots in a ring $\mathbb{Z}_m$ whenever the prime factorization of m is known. In Section 2, some general results on the subject are given. Peralta algorithms for square roots are generalized to cube roots in Section 3. In Section 4, the Tonelli and Shanks algorithm is generalized in the same way.

2. CUBE ROOT IN $\mathbb{Z}_m$

We wish to compute cube roots of $a \in \mathbb{Z}_m$, that is, we wish to solve the equation

$$x^3 \equiv a \bmod m.$$

Assume that the prime factorization of m is $m = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n}$. Using the *Chinese Remainder Theorem* the existence of cube roots on $\mathbb{Z}_m$ is equivalent to the existence of the roots on $\mathbb{Z}_{p_i^{r_i}}$

0893-9659/02/$ - see front matter Typeset by AMS-TEX

PII: S0893-9659(02)00031-9

for every $i = 1, \ldots, n$. This theorem provides a method for computing cube roots on $\mathbb{Z}_m$ from the roots on every $\mathbb{Z}_{p_i^{r_i}}$.

Hensel's lemma [7] give us a method that can be used to find cube roots in every $\mathbb{Z}_{p_i^{r_i}}$ if they are known in $\mathbb{Z}_{p_i}$.

The computation of cube roots in a $\mathbb{Z}_m$ for a composite m is then reduced to the computation of cube roots in $\mathbb{Z}_p$ for a prime p. When $a \equiv 0 \bmod p$ or $p = 2$ or $p = 3$ the equation $x^3 \equiv a \bmod p$ has an unique solution: $x \equiv a \bmod p$. If $a \not\equiv 0 \bmod p$, and $p \neq 2, 3$, two cases on p must be distinguished for the existence of cube roots and the discussion of the number of roots.

If $p \equiv -1 \bmod 3$ every number has one cube root and only one due to the fact that there is not any nontrivial cube roots of 1. In this case, the cube root is computed by

$$\sqrt[3]{a} = a^{(2p-1)/3}$$

or by the formula $\sqrt[3]{a} = \pm a^{(p+1)/6}$ where $\pm$ means that there is only one possibility that has to be checked. This root can be computed using the square-and-multiply algorithm in a running time $O(\log^3 p)$.

If $p \equiv 1 \bmod 3$, then -3 is a quadratic residue modulo p and $\epsilon = (-1 + \sqrt{-3})/2$ is a nontrivial cube root of 1. Then, it can be proved that one third of the $p - 1$ nonzero numbers have three cube roots and two thirds have no cube root. The existence of the cube roots depends on the value of the symbol $[a/p] = a^{(p-1)/3} \bmod p$ (multiplicative character). There exist cube roots for $a \not\equiv 0 \bmod p$ if and only if $[a/p] = 1$. If a cube root x_0 is known, the other ones are $x_0\epsilon$ and $x_0\epsilon^2$ verifying $x_0 + x_0\epsilon + x_0\epsilon^2 \equiv 0 \bmod p$. The other values of the symbol are ϵ and ϵ^2. One third of the nonzero numbers have 1 as symbol, the second third ϵ and the remaining third ϵ^2. For $p \equiv 1 \bmod 3$, there is no formula for every prime and every a as a power of a, because in some cases cube roots are not in the multiplicative subgroup generated by a. However, there are formulae for some cases; for instance, for $p \equiv 7 \bmod 9$

$$\sqrt[3]{a} = a^{(p+2)/9}.$$

In this paper, we generalize two of the fastest algorithms for computing square roots modulo a prime to algorithms for computing cube roots. The Peralta [4] randomized algorithm has been generalized in Section 3 using a ring analogous to the one constructed for square roots and with similar properties. This method allows us to compute cube roots in a fast way, particularly when $p = 3^e q + 1$ ($q \not\equiv 0 \bmod 3$) for big e. Two algorithms are proposed with running time $O(\log^3 p)$. The Tonelli-Shanks [1,3] algorithm is a group theory based method for finding square roots, which is generalized in Section 4 for the purpose of finding cube roots. The running time of this algorithm is $O(\log^4 p)$.

3. PERALTA METHOD EXTENSION

The Peralta method [4] is a fast way of computing square roots for a prime of the form $p = 2^e q + 1$ ($q \not\equiv 0 \bmod 2$) for large e. Two algorithms are constructed to compute cube roots for a prime of the form $p = 3^e q + 1$ ($q \not\equiv 0 \bmod 3$) for large e.

Consider a number $a \in \mathbb{Z}_p$ such that $[a/p] = 1$; that is, the cube root of a exists. Consider the ring

$$R = \frac{\mathbb{Z}_p[x]}{(x^3 - a)} = \left\{\alpha + \beta Y + \gamma Y^2 \mid \alpha, \beta, \gamma \in \mathbb{Z}_p\right\}$$

with the usual operations ($Y^3 = a$) and the direct product $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$. Then, we have the following proposition.

PROPOSITION 3.1. *R and $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ are isomorphic rings.*

PROOF. Consider $x_0 \in \mathbb{Z}_p$ a cube root of a, that is, $x_0^3 \equiv a \bmod p$ and the function $\varphi : R \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ defined by

$$\varphi\left(\alpha + \beta Y + \gamma Y^2\right) = \left(\alpha + \beta x_0 + \gamma x_0^2,\ \alpha + \beta\epsilon x_0 + \gamma\epsilon^2 x_0^2,\ \alpha + \beta\epsilon^2 x_0 + \gamma\epsilon x_0^2\right).$$

The linear system

$$\begin{aligned}\alpha + \beta x_0 + \gamma x_0^2 &\equiv x \bmod p,\\ \alpha + \beta\epsilon x_0 + \gamma\epsilon^2 x_0^2 &\equiv y \bmod p,\\ \alpha + \beta\epsilon^2 x_0 + \gamma\epsilon x_0^2 &\equiv z \bmod p,\end{aligned}$$

has a unique solution because the determinant of the system $3a(\epsilon - 1)$ is nonzero ($a \not\equiv 0 \bmod p$, $p \neq 2$ and $p \neq 3$). Then φ is a bijection. It is an isomorphism of rings, because it verifies $\varphi(z_1 + z_2) = \varphi(z_1) + \varphi(z_2)$, $\varphi(z_1 z_2) = \varphi(z_1)\varphi(z_2)$ for every $z_1, z_2 \in R$ and $\varphi(1) = (1,1,1)$. ∎

As a consequence of the isomorphism, *Fermat's little theorem* holds in R.

COROLLARY 3.2. *For every $z \in R^*$, $z^{p-1} = 1$.*

PROOF. If $\varphi(z) = (r,s,t)$ then $\varphi(z^{p-1}) = (r^{p-1}, s^{p-1}, t^{p-1}) = (1,1,1) = \varphi(1)$ and that is why $z^{p-1} = 1$. ∎

The first algorithm we propose uses this last corollary. If we know $z \in R^*$ in such a way that $z^{(p-1)/3} = \beta Y$ for some $\beta \in \mathbb{Z}_p$ then

$$\sqrt[3]{a} = \beta^{-1},$$

because if $z^{(p-1)/3} = \beta Y$ then $1 \equiv \beta^3 a \bmod p$ and $(\beta^{-1})^3 \equiv a \bmod p$.

The next algorithm is proposed to find a cube root of a cubic residue $a \in \mathbb{Z}_p$.

ALGORITHM 3.3. For a prime $p \equiv 1 \bmod 3$

Input: a cubic residue a modulo p

Output: $x \in \mathbb{Z}_p$ such that $x^3 \equiv a \bmod p$

(1) Choose $z \in R^*$ at random.
(2) Compute $z^{(p-1)/3} = \alpha + \beta Y + \gamma Y^2$.
(3) If $\alpha = \gamma = 0$, then write($\beta^{-1} \bmod p$) otherwise go to Step 1.

It is relevant to ask what the probability of a randomly chosen $z \in R^*$ verifying $z^{(p-1)/3} = \beta Y$ for some $\beta \in \mathbb{Z}_p$ might be.

PROPOSITION 3.4. $\Pr(z^{(p-1)/3} = \beta Y \text{ for some } \beta \in \mathbb{Z}_p \mid z \in R^*) = 1/9$.

PROOF. If $z \in R^*$ is such that $z^{(p-1)/3} = \beta Y$ for some $\beta \in \mathbb{Z}_p$, and $\varphi(z) = (r,s,t)$, then $(r^{(p-1)/3}, s^{(p-1)/3}, t^{(p-1)/3}) = (\beta x_0, \beta\epsilon x_0, \beta\epsilon^2 x_0)$. Since $r^{(p-1)/3}, s^{(p-1)/3}, t^{(p-1)/3} \in \{1, \epsilon, \epsilon^2\}$ the number β must be $\beta \equiv x_0^{-1}\epsilon^i \bmod p$ for some $i = 0,1,2$ and $[r/p] = \epsilon^i$, $[s/p] = \epsilon^{i+1}$, $[t/p] = \epsilon^{i+2}$. On the other hand, $z = \varphi^{-1}(r,s,t)$ with $[r/p] = \epsilon^i$, $[s/p] = \epsilon^{i+1}$, $[t/p] = \epsilon^{i+2}$ for $i = 0,1,2$ verifies $z^{(p-1)/3} = x_0^{-1}\epsilon^i Y$ because $\varphi(z^{(p-1)/3}) = (\epsilon^i, \epsilon^{i+1}, \epsilon^{i+2}) = \varphi(x_0^{-1}\epsilon^i Y)$. Then we have $3((p-1)/3)^3$ possible values for (r,s,t) among $(p-1)^3$ possible values of invertible elements. ∎

The probabilistic part of the algorithm has a high probability of success.

From the proof of Proposition 3.4 one may observe that for $i = 0$ one of the cube roots can be found, the second one for $i = 1$ and the last one for $i = 2$. That is why Algorithm 3.3 finds every cube root with the same probability. In order to find all the cube roots, we will iterate the algorithm until two different cube roots x_0, x_1 are found, and the third one can be computed as $x_2 = -x_0 - x_1$.

In order to determine when an element is invertible, we use the *conjugate* of a number $\alpha + \beta Y + \gamma Y^2$ with $\alpha, \beta, \gamma \in \mathbb{Z}_p$ as

$$\overline{\alpha + \beta Y + \gamma Y^2} = \alpha + \beta\epsilon Y + \gamma\epsilon^2 Y^2.$$

Using this ring isomorphism, the *norm* of a number of R is the element of $\mathbb{Z}_p$

$$N(z) = z \cdot \bar{z} \cdot \bar{\bar{z}}.$$

This application verifies that $N(z_1 z_2) = N(z_1)N(z_2)$ and we can check if an element is invertible with its norm in the following way: $z \in R^*$ if and only if $N(z) \neq 0$. Now we are able to translate Step 1 of the algorithm.

(1′) Choose $z \in R$ at random, such that $N(z) \neq 0$.

Observe that it is enough to choose z on Step (1) of the form $z = 1 + \beta Y + \gamma Y^2$.

The next proposition give us a faster algorithm.

PROPOSITION 3.5.

Let $z = \alpha + \beta Y + \gamma Y^2$ be an element of R with at least two nonzero coefficients

(1) *if $z^3 = \alpha'$ with $\alpha' \in \mathbb{Z}_p^*$, then*
   (1a) if $\beta, \gamma \not\equiv 0 \bmod p$, then $\sqrt[3]{a} = \alpha/\beta$,
   (1b) if $\beta \equiv 0 \bmod p, \alpha, \gamma \not\equiv 0 \bmod p$, then $\sqrt[3]{a} = (1/a)(\alpha/\gamma)^2$,
   (1c) if $\gamma \equiv 0 \bmod p, \alpha, \beta \not\equiv 0 \bmod p$, then $\sqrt[3]{a} = -\alpha/\beta$,
(2) *if $z^3 = \beta' Y$ with $\beta' \in \mathbb{Z}_p^*$, then $\sqrt[3]{a} = N(z)/\beta'$,*
(3) *if $z^3 = \gamma' Y^2$ with $\gamma' \in \mathbb{Z}_p^*$, then $\sqrt[3]{a} = (N(z))^2/(\gamma')^2 a$.*

PROOF 1.

(a) Since

$$z^3 = \left(\alpha + \beta Y + \gamma Y^2\right)^3$$
$$= \alpha^3 + \gamma^3 a^2 + a\left(6\alpha\beta\gamma + \beta^3\right) + 3\left(\left(\alpha\gamma^2 + \beta^2\gamma\right)a + \alpha^2\beta\right)Y + 3\left(\alpha^2\gamma + \alpha\beta^2 + \beta\gamma^2 a\right)Y^2,$$

is an element of $\mathbb{Z}_p^*$,

$$\left(\alpha\gamma^2 + \beta^2\gamma\right)a + \alpha^2\beta \equiv 0 \bmod p,$$
$$\alpha^2\gamma + \alpha\beta^2 + \beta\gamma^2 a \equiv 0 \bmod p$$

multiplying the first equation by β and subtracting the second multiplied by α, we have $\beta^3\gamma a - \alpha^3\gamma \equiv 0 \bmod p$, and then $a \equiv (\alpha/\beta)^3 \bmod p$ if $\beta, \gamma \neq 0 \bmod p$.

(b) If $z^3 = (\alpha + \gamma Y^2)^3 \in \mathbb{Z}_p^*$, conjugating $\bar{z}^3 = (\alpha + \gamma\epsilon^2 Y^2)^3 \in \mathbb{Z}_p^*$, then the product $z^3\bar{z}^3 = (\alpha^2 + \epsilon^2\gamma^2 aY + \alpha\gamma(1+\epsilon^2)Y^2)^3 \in \mathbb{Z}_p^*$, and using 1(a), we obtain the result.

(c) If $z^3 = (\alpha + \beta Y)^3 \in \mathbb{Z}_p^*$, conjugating $\bar{z}^3 = (\alpha + \beta\epsilon Y)^3 \in \mathbb{Z}_p^*$, then the product $z^3\bar{z}^3 = (\alpha^2 + (1+\epsilon)\alpha\beta Y + \beta^2\epsilon Y^2)^3 \in \mathbb{Z}_p^*$, and using 1(a), we obtain the result, since $1 + \epsilon \not\equiv 0 \bmod p$ ($p \neq 2$), and the inverse of $1 + \epsilon$ is $-\epsilon$.

PROOF 2. We have $z^3 = \beta' Y$, then $N(z^3) \equiv \beta'^3 a \bmod p$ and $a \equiv (N(z)/\beta')^3 \bmod p$.

PROOF 3. We have $z^3 = \gamma' Y^2$, then $(z^2)^3 = \gamma'^2 aY$. Using Proof 2, $\sqrt[3]{a} = N(z^2)/\gamma'^2 a = (N(z))^2/\gamma'^2 a$. ∎

Let $z \in R^*$ be an element with at least two nonzero coefficients and such that its cube has two coefficients equal to zero. As a consequence of Proposition 3.5, a cube root of a can be computed in terms of z and z^3. One option to find such a $z \in R^*$ is using the fact that $(z^q)^{3^e} = 1$, because Corollary 3.2 for $z \in R^*$. The procedure is to compute z^q, and after that cubing is repeated as many times as necessary until a cube with two zeros is found, and then Proposition 3.5 is used. Only when z^q has two zeros this method cannot be applied. The algorithm proposed here is the following.

ALGORITHM 3.6. For a prime $p = 3^e q + 1$ such that $q \not\equiv 0 \bmod 3$ with $e > 1$

Input: a cubic residue a modulo p

Output: $x \in \mathbb{Z}_p$ such that $x^3 \equiv a \bmod p$

(1) Choose $z \in R$ at random such that $N(z) \neq 0$ with no two coefficients equal to zero.
(2) Compute $z_1 := z^q$.

(3) If z_1 has two coefficients equal to zero, then go to 1.
(4) Compute $z_1^{3^i}$ for $i = 1, 2, \ldots$ by repeated cubing until $z_1^{3^i}$ has two coefficients equal to zero, then output a cube root applying formulae of Proposition 3.5 to $z_1^{3^{i-1}}$ and $z_1^{3^i}$.

What is the probability of z^q having two zeros for a random chosen $z \in R^*$?

PROPOSTIONS 3.7. *Let p be a prime such that $p = 3^e q + 1$ $(q \not\equiv 0 \bmod 3)$, then*

$$\Pr(z^q \text{ has at least two nonzero coefficients } \mid z \in R^*) = 1 - \frac{1}{3^{2e-1}}.$$

PROOF. Let $z \in R^*$ be an element such that z^q has two zeros. The corresponding element in $\mathbb{Z}_p^* \times \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ is $(r, s, t) = \varphi(z)$ with (r^q, s^q, t^q) equal to either (α, α, α) or $(\beta x_0, \beta x_0 \epsilon, \beta x_0 \epsilon^2)$ or $(\gamma x_0^2, \gamma x_0^2 \epsilon, ^2, \gamma x_0^2 \epsilon)$.

In the first case, $(r/t)^q \equiv 1, (s/t)^q \equiv 1 \bmod p$. Using the fact that $(\mathbb{Z}_p^*, \cdot)$ is isomorphic to $(\mathbb{Z}_{p-1}, +)$, we know that the equation $x^q \equiv 1 \bmod p$ has $\gcd(q, 3^e q) = q$ solutions $a_1, \ldots, a_q$. Then $(r, s, t) = (a_i t, a_j t, t)$ for $i, j = 1, \ldots, q$ and $t = 1, \ldots, p-1$ represent every element of R^*, such that $z^q \in \mathbb{Z}_p$. We have $q^2(p-1) = 3^e q^3$ different elements.

It is easy to check that the same computation is true in the second case when $(r/t)^q \equiv \epsilon$, $(s/t)^q \equiv \epsilon^2 \bmod p$, and in the third case when $(r/t)^q \equiv \epsilon^2$, $(s/t)^q \equiv \epsilon \bmod p$.

Summarizing, we have $3^{e+1} q^3$ different elements, and then the probability is $1 - 3^{e+1} q^3 / (3^e q)^3 = 1 - 1/3^{2e-1}$. ∎

The running time of the nonprobabilistic part of both algorithms is $O(\log^3 p)$, but the second algorithm is in general computationally more efficient.

4. TONELLI-SHANKS METHOD EXTENSION

A probabilistic algorithm for taking cube roots of a number analogous to the Tonelli-Shanks [1,3] for square roots is found.

Let p be a prime such that $p = 3^e q + 1 (q \not\equiv 0 \bmod 3)$. We know that $(\mathbb{Z}_p^*, \cdot)$ is isomorphic to $(\mathbb{Z}_{p-1}, +)$. Since $|\mathbb{Z}_{p-1}| = 3^e q$ there exists G the unique 3-Sylow subgroup [8], which is a subgroup G of 3^e elements which contains any subgroup of order divisor of 3^e. This fact can be expressed using a generator g as $G = \{g^i \mid 0 \le i < 3^e\}$, because it is cyclic. Using the next proposition, cube roots in terms of g can be found.

PROPOSITION 4.1. *Let p be a prime such that $p = 3^e q + 1$ $(q \not\equiv 0 \bmod 3)$ and $G = \langle g \rangle$ the unique 3-Sylow subgroup of $\mathbb{Z}_p^*$. There exist $0 \le k < 3^e$ such that if $q \equiv 1 \bmod 3$ then $\sqrt[3]{a} = a^{(2q+1)/3} g^k$, and if $q \equiv 2 \bmod 3$, then $\sqrt[3]{a} = a^{(q+1)/3} g^k$.*

PROOF. We may observe that an element is a cube in G if and only if the element order is a divisor of 3^{e-1}. Since $a^{(p-1)/3} \equiv 1 \bmod p$, then $(a^q)^{3^{e-1}} \equiv 1 \bmod p$ and the order of a^q is a divisor of 3^{e-1}; that is, a number of the form 3^i for some $i = 1, \ldots, e-1$. As a consequence, a^q is a cube in G and the 3-subgroup $\langle a^q \rangle$ generated by a^q is a subgroup of G, then $a^q \in G$. It follows that there exists a number $0 \le i < 3^e$ such that $a^q \equiv g^{3i} \bmod p$.

If $q \equiv 2 \bmod 3$, then $q + 1$ is a multiple of 3 and $a^{q+1} g^{-3i} \equiv a \bmod p$ can be rewritten as $(a^{(q+1)/3} g^{-i})^3 \equiv a \bmod p$, and then $\sqrt[3]{a} = a^{(q+1)/3} g^k$ for some k.

If $q \equiv 1 \bmod 3$, then $2q \equiv 2 \bmod 3$. Since $2q + 1$ is a multiple of 3 and $a^{2q} g^{-6i} \equiv 1 \bmod p$, then $a^{2q+1} g^{-6i} \equiv a \bmod p$ and $(a^{(2q+1)/3} g^{-2i})^3 \equiv a \bmod p$, so $\sqrt[3]{a} = a^{(2q+1)/3} g^k$ for some k. ∎

In order to find a generator of the group G, we will look for a noncubic residue $h \in \mathbb{Z}_p^*$; that is, $[h/p] \neq 1$. Consequently, $g = h^q$ is a generator of G: $g^{3^e} = h^{3^e q} = h^{p-1} \equiv 1 \bmod p$, but $g^{3^{e-1}} = h^{3^{e-1} q} = h^{(p-1)/3} = [h/p] \not\equiv 1 \bmod p$.

We propose the following algorithm.

ALGORITHMS 4.2. *For a prime $p = 3^e q + 1$ such that $q \not\equiv 0 \bmod 3$ with $e \geq 1$.*

Input: $a \in \mathbb{Z}_p$

Output: *All $x \in \mathbb{Z}_p$ such that $x^3 \equiv a \bmod p$ if x is a cubic residue, otherwise there is a nonexistence of cube root message.*

(1) *Find $h \in \mathbb{Z}_p$ at random such that $[h/p] \neq 1 \bmod p$.*

(2) *Initialize: $g := h^q$; symbol $:= [h/p]$; $y := g$; $r := e$; If $q \equiv 2 \bmod 3$ then $x := a^{(q-2)/3}$; otherwise $x := a^{(2q-2)/3}$ $b := a^2 x^3$; $x := ax$.*

(3) *Find exponent or finish. If $b \equiv 1 \bmod p$, then write $(x, x \cdot symbol, x \cdot symbol^2)$ and stop. Otherwise find $m := \min\{i \mid b^{3^i} \equiv 1 \bmod p\}$. If $m = r$ then write ('there is no cube root') and stop.*

(4) *Reduce exponent: if symbol $= b^{3^{m-1}}$ then $t := y^2$, symbol $:=$ symbol^2. Otherwise, $t := y$. $t := t^{3^{r-m-1}}$; $y := t^3$; $r := m$; $x := xt$; $b := by$; go to Step 3.*

It is easy to check that this algorithm computes six sequences defined by

$$r_{n+1} = \min\{i \mid b_n^{3^i} \equiv 1 \bmod p\}, \qquad t_{n+1} = y_n^{k_n 3^{r_n - r_{n+1} - 1}},$$
$$y_{n+1} = t_{n+1}^3, \qquad x_{n+1} = x_n t_{n+1}, \qquad b_{n+1} = b_n y_{n+1},$$

with $k_n = 2$ if $y_n^{3^{r_n-1}} \equiv b_n^{3^{r_{n+1}-1}} \bmod p$ and $k_n = 1$ otherwise; $x_1 = a^{(2q+1)/3}, b_1 = a^{2q}$ if $q \equiv 1 \bmod 3$ and $x_1 = a^{(q+1)/3}, b_1 = a^q$ if $q \equiv 2 \bmod 3$; $r_1 = e$, $y_1 = g$. They verify

$$ab_n \equiv x_n^3, \qquad y_n^{3^{r_n-1}} \equiv \epsilon \text{ or } \epsilon^2, \qquad b_n^{3^{r_n-1}} \equiv 1 \bmod p,$$

and the sequence of numbers r_n is strictly decreasing. For this reason, when r_n arrives to $r_n = 1$, b_n is 1 and x_n is such that $a \equiv x_n^3 \bmod p$. In fact, with this algorithm we can compute the value of the exponent k in Proposition 4.1 as $k = \sum_{i=2}^{n} k_1 \ldots k_{i-1} 3^{e-r_i-1}$.

If we call G_r to the subgroup of the elements with order divisor of 3^r, we have $G_r = \langle y \rangle$ and $b \in G_{r-1}$. The sequence of subgroups G_r is strictly decreasing, $G_r \subset G_{r-1}$ with length shorter than e, and when $r = 1$ the corresponding subgroup is $G_r = \{1\}$.

The only probabilistic part of the algorithm is Step 1. The probability of finding a noncubic residue in $\mathbb{Z}_p^*$ is 2/3, a very high probability. The number of loops of Steps 3 and 4 is at most e times. The running time of this algorithm is $O(\log^4 p)$ because the running time of one multiplication with a modular reduction is $O(\log^2 p)$.

REFERENCES

1. H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics 138, Springer-Verlag, Berlin, (1995).
2. L. Adleman, K. Manders and G. Miller, On taking roots in finite fields, presented at 18th IEEE Annual Symp. Foundations of Computer Science, Providence, RI, (1977).
3. D. Shanks, Five number-theoretical algorithms, In *Proc. Second Manitoba Conf. on Numerical Mathematics*, University of Manitoba, Winnipeg, Manitoba, Canada, (1972).
4. R.C. Peralta, A simple and fast probabilistic algorithm for computing square roots modulo a prime number, *IEEE Transactions on Information Theory* **IT-32** (6), 846–847, (November 1986).
5. R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **43**, 483–494, (1985).
6. D.H. Lehmer, Computer technology applied to the theory of numbers, In *Studies in Number Theory*, (Edited by W.J. LeVeque) MAA, Prentice Hall, Englewod Cliffs, NJ, (1969).
7. I. Niven and H.S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley and Sons, New York, (1966).
8. S. Lang, *Algebra*, Addison-Wesley, (1971).