Annales UMCS Informatica AI XI, 2 (2011)
113–125; DOI: 10.2478/v10065-011-0008-5

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI

http://www.annales.umcs.lublin.pl/

Generating elements of orders dividing $p^6 \pm p^5 + p^4 \pm p^3 + p^2 \pm p + 1$

Maciej Grześkowiak*

Adam Mickiewicz University, Faculty of Mathematics and Computer Science
Umultowska 87, 61-614 Poznań, Poland

Abstract

In this paper we propose an algorithm for computing large primes p and q such that q divides $p^6 + p^5 + p^4 + p^3 + p^2 + p + 1$ or $p^6 - p^5 + p^4 - p^3 + p^2 - p + 1$. Such primes are the key parameters for the cryptosystem based on the 7th order characteristic sequences.

1. Introduction

Let Φ_n be the nth cyclotomic polynomial; this is a unique monic polynomial whose roots are the primitive nth roots of unity. Algorithms for computing primes p and q such that q divides $\Phi_n(p)$ play an important role in cryptography. They are utilized for computing key parameters in cryptosystems which work in an extension of finite field $\mathbf{F}_p$. These systems reduce representations of finite field elements by representing them with the coefficients of their minimal polynomials. The examples of such systems are XTR [**1**], GH [**2**], [**3**], GG [**4**]. In [**5**] a general class of cryptographic schemes based on nth order characteristic sequences generated by an LFSR has been proposed. In order to generate key parameters for the cryptosystem based on nth order characteristic sequences

**E-mail address: maciejg@amu.edu.pl*
The author was partially supported by the grant no. N N201 6059 40 from National Science Centre.

one should find a large prime p and an element $\alpha \in \mathbf{F}_{p^n}$ of order q dividing $\Phi_n(p)$. One can determine whether or not the element α has the desired order if one knows the primes q and p such that q divides $\Phi_n(p)$. A method for finding the element α has not been given in [**5**]. From the security point of view it is essential to find a prime p such that $\Phi_n(p)$ has a large prime factor q having at least 160 bits to make DLP Problem in the subgroup of order q of $\mathbf{F}_{p^n}$ intractable. Moreover, one should find a prime p such that $n \log p \approx 2048$ to obtain security equivalent to factoring a positive integer having 2048 bits.

We propose a new method of finding primes p and q such that q divides $\Phi_7(p)$ or $\Phi_{14}(p)$. In particular, we present a new, deterministic algorithm for finding roots of polynomials $\Phi_7(x)$ or $\Phi_{14}(x) \pmod q$. Our method of finding the roots reduces to performing only exponentiations, multiplications and computing inversion modulo q. Achieving the described goals is made possible by generating the prime q, which is a norm of an algebraic integer of ring of some cubic algebraic number field.

The rest of this paper is organized as follows. In Section 2 we introduce the notation used throughout the paper. Section 3 presents our algorithm. In Section 4 we prove the correctness of the algorithm.

2. Notations

Throughout this paper, $K = Q(\eta_1) = \{x + y\eta_1 + z\eta_2 : x, y, z \in Q\}$ denotes the cubic number field with the ring of integers $\mathcal{O}_K = \{a + b\eta_1 + c\eta_2 : a, b, c \in Z\}$. Let ξ_7 be a primitive 7th root of unity. The field K is obtained from Q by adjoining $\eta_1 = \xi_7 + \xi_7^{-1}$ the root of irreducible over the rationals polynomial $f(x) = x^3 + x^2 - 2x - 1$. We will denote by $\eta_2 = \xi_7^2 + \xi_7^{-2}$ and $\eta_2 = \xi_7^3 + \xi_7^{-3}$ the second and the third roots of $f(x)$. The symbol $N(\alpha)$ will denote the norm of any element $\alpha \in K$ with respect to Q; that is the product of all algebraic conjugates of α.

3. The Algorithm

Let us fix $n = 7$ or $n = 14$. We describe an algorithm which generates primes p and q such that q divides $\Phi_n(p)$. The algorithm consists of the three following procedures.

Procedure FindPrimeQ(k, l, m). Let us fix $k, l, m \in Z$, $(k, l, m) = 1$, $|N(k + l\eta_1 + m\eta_2)| \equiv 15 \pmod{28}$, where $k + l\eta_1 + m\eta_2 \in \mathcal{O}_K$. This procedure finds $a + b\eta_1 + c\eta_2 \in \mathcal{O}_K$, where $a \equiv k \pmod{28}$, $b \equiv l \pmod{28}$, $c \equiv m \pmod{28}$ such that $|N(a + b\eta_1 + c\eta_2)| = q$ is a prime.

(1) Choose $a+b\eta_1+c\eta_2$ at random in $\mathcal{O}_K$ such that $a \equiv k \pmod{28}$, $b \equiv l \pmod{28}$, $c \equiv m \pmod{28}$.
(2) Compute $q = |N(a + b\eta_1 + c\eta_2)|$. If q is a prime, then terminate the procedure. Otherwise go to step 1.
(3) Return a, b, c and q.

Procedure FindRootOfFModQ(a, b, q). Let $n = 7$ or $n = 14$. Given a prime q and a, b, c such that $q = |N(a + b\eta_1 + c\eta_2)| \equiv 15 \pmod{28}$, this procedure computes r a root of $\Phi_n(x)$ modulo q.

(1) Compute $A \equiv (-b^2+2c^2+a^2+2ab-3ac-4cb) \pmod{q}$. If $(A, q) = 1$, then $B = b^2 + 2c^2 + 2ab - ac - 3cb$ and go to step 3. Otherwise go to step 2.
(2) Compute $A \equiv (-a^2+2ac+cb) \pmod{q}$ and $B = -a^2+c^2+ab+ac-bc$.
(3) Compute $s \equiv (-B)A^{-1} \pmod{q}$.
(4) Compute $t \equiv (s^2 - 4)^{(q+1)/4} \pmod{q}$
(5) Compute $w \equiv (s - t)2^{-1} \pmod{q}$
(6) If $n = 7$, then $r = w$. If $n = 14$, then $r \equiv -w \pmod{q}$.
(7) Return r.

Procedure FindPrimeP(r, q). Given a prime q and $r < q$, this procedure finds a prime $p \equiv r \pmod{q}$.

(1) Choose randomly $v \in N$.
(2) Compute $p = qv + r$. If p is a prime, then terminate the procedure. Otherwise go to step 1.
(3) Return p.

Algorithm 1. Generating primes p and q, such that $q|\Phi_n(p)$
Input: $k, l, m \in N : (k, l, m) = 1$, $|N(k + l\eta_1 + m\eta_2)| \equiv 15 \pmod{28}$, $n = 7$ or $n = 14$.
Output: Primes p and q such that $q|\Phi_n(p)$.

1 FindPrimeQ(k, l, x);
2 FindRootModuloQ(a, b, c, q, n);
3 FindPrimeP(r, q);

4 **Return** p, q;

4. Correctness of the Algorithm

Theorem 1. *Let us fix $n = 7$ or $n = 14$. Then Algorithm 1 generates primes p and q such that q divides $\Phi_n(p)$.*

Proof. We begin by proving auxiliary lemmas.

Lemma 1. *Let ξ_7 be a primitive 7th root of unity and let $f(x) = x^3 + x^2 - 2x - 1 \in Z[x]$. Then $f(x)$ is the minimal polynomial of $\eta_i = \xi_7^i + \xi_7^{-i}$.*

Proof. A short computation shows that

$$f(x) = (x - \eta_1)(x - \eta_2)(x - \eta_3) =$$
$$= x^3 - (\eta_1 + \eta_2 + \eta_3)x^2 + (\eta_1\eta_2 + \eta_1\eta_3 + \eta_2\eta_3)x - \eta_1\eta_2\eta_3.$$

We shall compute the coefficients of $f(x)$. We have

$$\Phi_7(\xi_7) = \xi_7^6 + \xi_7^5 + \xi_7^4 + \xi_7^3 + \xi_7^2 + \xi_7 + 1 = 0,$$

dividing by ξ_7^3 we obtain

$$\xi_7^3 + \xi_7^2 + \xi_7 + 1 + \xi_7^{-1} + \xi_7^{-2} + \xi_7^{-3} = 0.$$

Thus

$$\eta_1 + \eta_2 + \eta_3 = -1. \tag{1}$$

A small computation yields

$$\eta_1\eta_2 = (\xi_7 + \xi_7^{-1})(\xi_7^2 + \xi_7^{-2}) = \xi_7^3 + \xi_7^{-1} + \xi_7 + \xi_7^{-3} = \eta_3 + \eta_1,$$

so

$$\eta_1\eta_2\eta_3 = \eta_3^2 + \eta_1\eta_3 = \eta_1 + 2 + \eta_1\eta_3 = 2 + \eta_1 + \eta_2 + \eta_3 = 1. \tag{2}$$

Likewise,

$$\eta_1\eta_2 + \eta_1\eta_3 + \eta_2\eta_3 = 2(\eta_1 + \eta_2 + \eta_3) = -2. \tag{3}$$

Note that $\eta_j = e^{2j\pi i/7} + e^{-2j\pi i/7} \in R$, so $f(x)$ is the minimal polynomial of η_i. This finishes the proof. $\square$

Lemma 2. *Let $\alpha = a + b\eta_1 + c\eta_2 \in \mathcal{O}_K$, where $\eta_i = \xi_7^i + \xi_7^{-i}$, $i = 1, 2$. Then*

$$N(\alpha) = a^3 + b^3 + c^3 - a^2b - a^2c - 2b^2a + 3b^2c - 2c^2a - 4c^2b + 3abc.$$

Proof. We have

$$\begin{aligned} N(\alpha) &= (a+b\eta_1+c\eta_2)(a+b\eta_2+c\eta_3)(a+b\eta_3+c\eta_1)\\ &= a^3+(b^3+c^3)(\eta_1\eta_2\eta_3)+(a^2b+a^2c)(\eta_1+\eta_2+\eta_3)+\\ &+ (b^2a+c^2a)(\eta_1\eta_2+\eta_1\eta_3+\eta_2\eta_3)+b^2c(\eta_1^2\eta_2+\eta_1\eta_3^2+\eta_2^2\eta_3)+\\ &+ c^2b(\eta_1\eta_2^2+\eta_1^2\eta_3+\eta_2\eta_3^2)+abc(\eta_1\eta_2+\eta_1\eta_3+\eta_2\eta_3+\eta_1^2+\eta_2^2+\eta_3^2),\end{aligned}$$

where $\eta_3=\xi_7^3+\xi_7^{-3}$. A short computation shows that

$$\eta_i^2=\eta_{i+1 \bmod 3}+2,$$

and so

$$\eta_1^2\eta_2+\eta_1\eta_3^2+\eta_2^2\eta_3=3(\eta_1+\eta_2+\eta_3)+6$$

and

$$\eta_1\eta_2^2+\eta_1^2\eta_3+\eta_2\eta_3^2=\eta_1\eta_2+\eta_1\eta_3+\eta_2\eta_3-2(\eta_1+\eta_2+\eta_3).$$

By the above and (1), (2), (3), the assertion follows. This finishes the proof. □

For any integers a,b,c we define the numbers

$$\begin{aligned} &A_1=-b^2+2c^2+a^2+2ab-3ac-4cb, && B_1=b^2+2c^2+2ab-ac-3cb,\\ &A_2=-a^2+2ac+cb, && B_2=-a^2+c^2+ab+ac-bc,\\ &A_3=a^2-b^2+c^2+ab-2ac-2bc, && B_3=c^2+ab-ac-2bc,\\ &C_1=a^2-3b^2-c^2-ab+2ac+4bc, && D_1=-b^2-c^2-ab+2ac+3bc,\\ &C_2=-a^2+2b^2-bc, && D_2=b^2-a^2+ac,\\ &C_3=a^2-2b^2-c^2-ab+ac+3bc, && D_3=-b^2+ac+bc\\ &E_1=a^2-4b^2+c^2+ab+ac+bc, && F_1=-b^2+c^2+ab-bc,\\ &E_2=-a^2-b^2-bc+ab, && F_2=-a^2+2ab+bc,\\ &E_3=a^2-2b^2-2c^2-2ab+2ac+5bc, && F_3=-c^2+ab+ac+2bc.\end{aligned} \tag{4}$$

With the notation as above

Lemma 3. *Let $\alpha=a+b\eta_1+c\eta_2\in\mathcal{O}_K$, where $|N(\alpha)|$ is a prime. Assume that, there exists $\beta\in\mathcal{O}_K$, $\beta=r+(-r-1)\eta_1+r\eta_2$, where $r\in Z$ such that $N(\alpha)$ divides $N(\beta)$. Then $rA_i+B_i\equiv 0 \pmod{|N(\alpha)|}$ or $rC_i+D_i\equiv 0 \pmod{|N(\alpha)|}$ or $rE_i+F_i\equiv 0 \pmod{|N(\alpha)|}$, where $i=1,2,3$. Moreover, there exists $j,k\in\{1,2,3\}$, $j\neq k$ such that the numbers A_j, A_k, C_j, C_k, E_j, E_k are prime to $N(\alpha)$.*

Proof. Let $N(\beta)=\beta_1\beta_2\beta_3$, where $\beta=\beta_1$ and β_i are all algebraic conjugates of β. Since $|N(\alpha)|$ is a prime, hence α is a prime element of $\mathcal{O}_K$ and hence $\alpha|\beta_1$ or $\alpha|\beta_2$ or $\alpha|\beta_3$, so we have three cases.

Case I: $\alpha|\beta_1$. Hence, there exists $\gamma \in \mathcal{O}_K$, $\gamma = x + y\eta_1 + z\eta_2$, $x, y, z \in \mathbf{Z}$ such that

$$(a + b\eta_1 + c\eta_2)(x + y\eta_1 + z\eta_2) = r + (-r - 1)\eta_1 + r\eta_2.$$

Hence we can consider the linear system of equations

$$\begin{cases} ax + (2b - c)y + (c - b)z = r, \\ bx + ay - cz = -r - 1, \\ cx + (b - c)y + (a - b - c)z = r, \end{cases} \tag{5}$$

which in the matrix form is

$$MX = R,$$

where

$$M = \begin{bmatrix} a & 2b - c & c - b \\ b & a & -c \\ c & b - c & a - b - c \end{bmatrix}, \quad X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \quad R = \begin{bmatrix} r \\ -r - 1 \\ r \end{bmatrix}.$$

We shall show that the matrix M is invertible. Let's compute $\det M$. We have

$$\det M = a \det M_{11} + (c - 2b) \det M_{12} + (c - b) \det M_{13}.$$

A short computation shows that

$$\begin{aligned} \det M_{11} &= a^2 - ab - ac + bc - c^2, \\ \det M_{12} &= -b^2 + c^2 + ab - bc, \\ \det M_{13} &= b^2 - ac - bc, \end{aligned}$$

and so

$$\det M = a^3 + b^3 + c^3 - a^2 b - a^2 c - 2b^2 a + 3b^2 c - 2c^2 a - 4c^2 b + 3abc.$$

By (2) we obtain $\det M = N(\alpha) \neq 0$. This proves the last claim. Hence x, y and z can be found with the Cramer's rule as

$$x = \frac{\det M_1}{\det M}, \quad y = \frac{\det M_2}{\det M}, \quad z = \frac{\det M_3}{\det M},$$

where M_i is the matrix formed by replacing the ith column of M by the column vector R. It is an elementary check that

$$\begin{aligned} x &= \frac{1}{N(\alpha)}(rA_1 + B_1), \\ y &= \frac{1}{N(\alpha)}(rA_1 + B_2), \\ z &= \frac{1}{N(\alpha)}(rA_3 + B_3), \end{aligned} \tag{6}$$

where A_i and B_i are defined by (4). Since $x, y, x \in Z$, so by (6)

$$\begin{array}{rcll} rA_1 + B_1 & \equiv & 0 & (\mathrm{mod}\ |N(\alpha)|), \\ rA_2 + B_2 & \equiv & 0 & (\mathrm{mod}\ |N(\alpha)|), \\ rA_3 + B_3 & \equiv & 0 & (\mathrm{mod}\ |N(\alpha)|). \end{array} \tag{7}$$

This proves the first assertion of the lemma for this case. We shall prove the second assertion of the lemma for this case. Firstly, we shall show that at least one of the numbers A_i is not divided by $N(\alpha)$. A short calculation shows that

$$\begin{array}{rcl} N(\alpha)^2 & = & N(a + b\eta_1 + c\eta_2) = \\ & = & (a^3 + b^3 + c^3 - a^2b - a^2c - 2b^2a + 3b^2c - 2c^2a - 4c^2b + 3abc)^2 \\ & = & N(A_1 + A_2\eta_1 + A_3\eta_2). \end{array}$$

Now, assume that $N(\alpha)$ divides the numbers A_i simultaneously. Then

$$N(A_1 + A_2\eta_1 + A_3\eta_2) = kN(\alpha)^3, \quad k \in Z,$$

but this contradicts the fact that $N(A_1 + A_2\eta_1 + A_3\eta_2) = N(\alpha)^2$. This proves the last claim. Secondly, we shall show that at least two of the numbers A_i are not divided by $N(\alpha)$. Without loss of generality we can assume that $N(\alpha)$ does not divide A_1. Then we have

$$N(\alpha)^2 = N(A_1 + A_2\eta_1 + A_3\eta_2) = A_1^3 + kN(\alpha), \quad k \in Z,$$

and hence $N(\alpha)|A_1$, which is a contradiction. This proves the last claim and the second assertion holds.

Case II: $\alpha|\beta_2$. A short computation shows that $\alpha = a - b + (c - b)\eta_2 - b\eta_3$. If $\alpha|\beta_2$, then there exists $\gamma \in \mathcal{O}_K$, $\gamma = x + y\eta_2 + z\eta_3$, $x, y, z \in \mathbf{Z}$ such that

$$(a - b + (c - b)\eta_2 - b\eta_3)(x + y\eta_1 + z\eta_2) = r + (-r - 1)\eta_2 + r\eta_3.$$

Hence we can consider the linear system of equations

$$\left\{ \begin{array}{l} (a - b)x + (2c - b)y - cz = r, \\ (c - b)x + (a - b)y + bz = -r - 1, \\ -bx + cy + (a + b - c)z = r, \end{array} \right. \tag{8}$$

which in the matrix form is

$$M = \begin{bmatrix} a - b & 2c - b & -c \\ c - b & a - b & b \\ -b & c & a + b - c \end{bmatrix}, \quad X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \quad R = \begin{bmatrix} r \\ -r - 1 \\ r \end{bmatrix}.$$

Hence

$$MX = R.$$

We shall show that the $\det M = N(\alpha) \neq 0$. We have

$$\det M = (a-b)\det M_{11} + (b-2c)\det M_{12} - c\det M_{13}.$$

A short computation shows that

$$\begin{aligned} \det M_{11} &= a^2 - ac - b^2, \\ \det M_{12} &= -c^2 + a(c-b) + 2bc, \\ \det M_{13} &= c^2 + b(a-c) - b^2, \end{aligned}$$

and so

$$\det M = a^3 + b^3 + c^3 - a^2b - a^2c - 2b^2a + 3b^2c - 2c^2a - 4c^2b + 3abc.$$

By (2) we obtain $\det M = N(\alpha) \neq 0$. This proves the last claim. Hence x, y, z can be found with the Cramer's rule as

$$x = \frac{\det M_1}{\det M}, \quad y = \frac{\det M_2}{\det M}, \quad z = \frac{\det M_3}{\det M},$$

where M_i is the matrix formed by replacing the ith column of M by the column vector R. It is an elementary check that

$$\begin{aligned} x &= \frac{1}{N(\alpha)}(rC_1 + D_1), \\ y &= \frac{1}{N(\alpha)}(rC_2 + D_2), \\ z &= \frac{1}{N(\alpha)}(rC_3 + D_3), \end{aligned} \tag{9}$$

where C_i and D_i are defined by (4). Since $x, y, x \in Z$, so by (9)

$$\begin{aligned} rC_1 + D_1 &\equiv 0 \pmod{|N(\alpha)|}, \\ rC_2 + D_2 &\equiv 0 \pmod{|N(\alpha)|}, \\ rC_3 + D_3 &\equiv 0 \pmod{|N(\alpha)|}. \end{aligned} \tag{10}$$

This proves the first assertion of the lemma for this case. We shall prove the second assertion of the lemma for this case. Firstly, we shall show that at least one of the numbers C_i is not divided by $N(\alpha)$. Similarly to the case I, a short calculation shows that

$$N(\alpha)^2 = N(C_1 + C_2\eta_1 + C_3\eta_2).$$

Now, assume that $N(\alpha)$ divides the numbers C_i simultaneously. Then

$$N(C_1 + C_2\eta_1 + C_3\eta_2) = kN(\alpha)^3, \quad k \in Z,$$

but this contradicts the fact that $N(C_1 + C_2\eta_1 + C_3\eta_2) = N(\alpha)^2$. This proves the last claim. Secondly, we shall show that at least two of the numbers C_i are not divided by $N(\alpha)$. Without loss of generality we can assume that $N(\alpha)$ does not divide C_1. Then we have

$$N(\alpha)^2 = N(C_1 + C_2\eta_1 + C_3\eta_2) = C_1^3 + kN(\alpha), \quad k \in Z,$$

and hence $N(\alpha)|C_1$, which is a contradiction. This proves the last claim and the second assertion holds.

Case III: $\alpha|\beta_3$. A short computation shows that $\alpha = a - c + (b - c)\eta_1 - c\eta_3$. If $\alpha|\beta_2$, then there exists $\gamma \in \mathcal{O}_K$, $\gamma = x + y\eta_2 + z\eta_3$, $x, y, z \in \mathbf{Z}$ such that

$$(a - c + (b - c)\eta_1 - c\eta_3)(x + y\eta_1 + z\eta_3) = r + (-r - 1)\eta_1 + r\eta_3.$$

Hence we can consider the linear system of equations

$$\begin{cases} (a-c)x + by - (c+b)z = r, \\ (b-c)x + (a-b+c)y - bz = -r-1, \\ -cx + (c-b)y + (a-c)z = r, \end{cases} \tag{11}$$

which in the matrix form is

$$M = \begin{bmatrix} a-c & b & -c-b \\ b-c & a-b+c & -b \\ -c & c-b & a-c \end{bmatrix}, \quad X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \quad R = \begin{bmatrix} r \\ -r-1 \\ r \end{bmatrix}.$$

Hence

$$MX = R.$$

We shall show that the $\det M = N(\alpha) \neq 0$. We have

$$\det M = (a - c)\det M_{11} - b \det M_{12} - (c + b)\det M_{13}.$$

A short computation shows that

$$\begin{aligned} \det M_{11} &= a^2 - b^2 - c^2 - ab + 2bc, \\ \det M_{12} &= -c^2 + a(b - c) - 2bc, \\ \det M_{13} &= b^2 + ac + bc, \end{aligned}$$

and so

$$\det M = a^3 + b^3 + c^3 - a^2b - a^2c - 2b^2a + 3b^2c - 2c^2a - 4c^2b + 3abc.$$

By (2) we obtain $\det M = N(\alpha) \neq 0$. Hence x, y and z can be found with the Cramer's rule as

$$x = \frac{\det M_1}{\det M}, \quad y = \frac{\det M_2}{\det M}, \quad z = \frac{\det M_3}{\det M},$$

where M_i is the matrix formed by replacing the ith column of M by the column vector R. It is an elementary check that

$$\begin{aligned} x &= \frac{1}{N(\alpha)}(rE_1 + F_1), \\ y &= \frac{1}{N(\alpha)}(rE_2 + F_2), \\ z &= \frac{1}{N(\alpha)}(rE_3 + F_3), \end{aligned} \tag{12}$$

where E_i and F_i are defined by (4). Since $x, y, x \in Z$, so by (12)

$$\begin{aligned} rE_1 + F_1 &\equiv 0 \pmod{|N(\alpha)|}, \\ rE_2 + F_2 &\equiv 0 \pmod{|N(\alpha)|}, \\ rE_3 + F_3 &\equiv 0 \pmod{|N(\alpha)|}. \end{aligned} \tag{13}$$

This proves the first assertion of the lemma for this case. We shall prove the second assertion of the lemma for this case. Firstly, we shall show that at least one of the numbers E_i is not divided by $N(\alpha)$. Similarly to cases I, II, a short calculation shows that

$$N(\alpha)^2 = N(E_1 + E_2\eta_1 + E_3\eta_2).$$

Now, assume that $N(\alpha)$ divides the numbers E_i simultaneously. Then

$$N(E_1 + E_2\eta_1 + E_3\eta_2) = kN(\alpha)^3, \quad k \in Z,$$

but this contradicts the fact that $N(E_1 + E_2\eta_1 + E_3\eta_2) = N(\alpha)^2$. This proves the last claim. Secondly, we shall show that at least two of the numbers E_i are not divided by $N(\alpha)$. Without loss of generality we can assume that $N(\alpha)$ does not divide A. Then we have

$$N(\alpha)^2 = N(E_1 + E_2\eta_1 + E_3\eta_2) = E_1^3 + kN(\alpha), \quad k \in Z,$$

and hence $N(\alpha)|E_1$, which is a contradiction. This proves the last claim and the second assertion holds. This finishes the proof. □

Lemma 4. *Let* $q \equiv \pm 1 \pmod 7$ *be a prime. Then the congruence*

$$f(r) = r^3 + r^2 - 2r - 1 \equiv 0 \pmod q \tag{14}$$

is solvable.

Proof. By Lemma 1 $f(x)$ is the minimal polynomial of $\eta_i = \xi_7 + \xi_7^{-i}$, $i = 1, 2, 3$. Let $K = Q(n_1)$ be the algebraic number field with the ring of integer $\mathcal{O}_K$, so $Q \subset K$ is the Galois extension. Let p be a prime not dividing $\Delta(f)$ discriminant of f, that is $p \neq 7$. The congruence $f(x) \equiv 0 \pmod p$ has a solution in Z if and only if the ideal $p\mathcal{O}_K$ splits completely in K (see [**6**], Proposition 5.11, page 102). Let $\mathfrak{p}$ be a prime ideal of K containing $p\mathcal{O}_K$ then $p\mathcal{O}_K$ splits completely in K if and only if the symbol Artin $\left(\frac{K/Q}{\mathfrak{p}}\right) = 1$ (see [**6**], Corollary 5.21, page 107). We shall compute

$$\left(\frac{K/Q}{\mathfrak{p}}\right)(\alpha), \quad \alpha = \alpha^p \equiv a + b\eta_1 + c\eta_2 \in \mathcal{O}_K.$$

We have

$$\left(\frac{K/Q}{\mathfrak{p}}\right)(\alpha) \equiv \alpha^p \equiv a + b\eta_1^p + c\eta_2^p \pmod{\mathfrak{p}}.$$

On the other hand

$$\eta_i^p = \xi_7^{ip} + \xi_7^{-ip} = \begin{cases} \xi_7^i + \xi_7^{-i} = \eta_i, & \text{for} \quad p \equiv \pm 1 \pmod 7 \\ \xi_7^{2i} + \xi_7^{-2i} = \eta_{i+1}, & \text{for} \quad p \equiv \pm 2 \pmod 7 \\ \xi_7^{3i} + \xi_7^{-3i} = \eta_{i+2}, & \text{for} \quad p \equiv \pm 3 \pmod 7 \end{cases},$$

where $i = 1, 2, 3$. Hence

$$\left(\frac{K/Q}{\mathfrak{p}}\right)(\alpha) \equiv \alpha \pmod{\mathfrak{p}}, \quad \text{for} \quad p \equiv \pm 1 \pmod 7,$$

and consequently the solution of (14) exists. This finishes the proof. □

Lemma 5. *Let $\alpha = a + b\eta_1 + c\eta_2 \in \mathcal{O}_K$, where $|N(\alpha)| \equiv \pm 1 \pmod 7$ and assume that $|N(\alpha)|$ is a prime. Then the congruence*

$$f(r) = r^3 + r^2 - 2r - 1 \equiv 0 \pmod q \tag{15}$$

is solvable and the solutions r_i, $i = 1, 2, 3$ satisfy

$$\begin{array}{llcll} r_1 A_1 \equiv -B_1 & (\text{mod } |N(\alpha)|) & \textit{or} & r_1 A_2 \equiv -B_2 & (\text{mod } |N(\alpha)|), \\ r_2 C_1 \equiv -D_1 & (\text{mod } |N(\alpha)|) & \textit{or} & r_2 C_2 \equiv -D_2 & (\text{mod } |N(\alpha)|), \\ r_3 E_1 \equiv -F_1 & (\text{mod } |N(\alpha)|) & \textit{or} & r_3 E_2 \equiv -F_2 & (\text{mod } |N(\alpha)|), \end{array}$$

where $A_j, B_j, C_j, D_j, E_j, F_j$ are defined by (4). Moreover, at least one of the numbers A_j, and at least one of C_j, and at least one of E_j is prime to $N(\alpha)$.

Proof. Let $\eta_i = \xi_7^i + \xi_7^{-i}$. By Lemma 4 solution of (15) exists and so by (1) η_i modulo $|N(\alpha)|$ exists. We have

$$\begin{aligned} 0 &\equiv r_i^3 + r_i^2 - 2r_i - 1 \pmod{|N(\alpha)|} \\ &\equiv (r - (r+1)\eta_1 + r\eta_2)(r - (r+1)\eta_2 + r\eta_3)(r - (r+1)\eta_3 + r\eta_1) \pmod{|N(\alpha)|} \\ &\equiv N(\beta) \pmod{|N(\alpha)|}, \end{aligned}$$

where $\beta = (r - (r+1)\eta_1 + r\eta_2) \pmod{|N(\alpha)|}$. Hence $N(\alpha)|N(\beta)$. Since β can be considered as an element of $\mathcal{O}_K$, then Lemma 3 shows that the assertion of the Lemma follows. This finishes the proof. □

Proof of Theorem 1. Let us assume that a, b, c and q are the output of procedure FindPrimeQ. Then $q \equiv 15 \pmod{28}$ is a prime such that $q = |N(a + b\eta_1 + c\eta_2)|$ and $a \equiv k \pmod{28}$, $b \equiv l \pmod{28}$, $c \equiv m \pmod{28}$. We shall show that the procedure FindRootModuloQ, with the input a, b, c, q and $n = 7$ or 14, computes r such that $\Phi_n(r) \equiv 0 \pmod{q}$. Firstly, suppose that $n = 7$. It is an elementary check that $q \equiv 1 \pmod{7}$. Lemma 5 shows that the solutions s_i of $f(x) = x^3 + x^2 - 2x - 1 \equiv \pmod{q}$ exists and one of them $s = s_1$ satisfy

$$sA_1 \equiv -B_1 \pmod{|N(\alpha)|} \quad \text{and} \quad sA_2 \equiv -B_2 \pmod{|N(\alpha)|},$$

and at least one of the numbers A_1, A_2 is prime to q. Without loss of generality we can assume that $(A, q) = 1$, where $A = A_1$ and hence $s \equiv (-B)A^{-1} \pmod{q}$, where $B = B_1$. By Lemma 1, $s \equiv \xi_7 + \xi_7^{-1} \pmod{q}$ or $s \equiv \xi_7^2 + \xi_7^{-2} \pmod{q}$ or $s \equiv \xi_7^3 + \xi_7^{-3} \pmod{q}$. Note that ξ_7^i, ξ_7^{-i}, $i = 1, 2, 3$ are the roots of $g(x) = x^2 - sx + 1 \pmod{q}$ and one of them is equal to $(s + \sqrt{(s^2 - 4)})/2 \pmod{q}$. We shall show that $s^2 - 4$ is a quadratic residue modulo q. Indeed, $q \equiv 1 \pmod{7}$, so ξ_7 modulo q exists, and hence $\xi_7 \in \mathbf{F}_q$. Suppose that $s^2 - 4$ is the quadratic nonresidue modulo q, then $g(x)$ is the irreducible modulo q, and so $\xi_7 \in \mathbf{F}_{q^2} \backslash \mathbf{F}_q$. This contradicts the fact that $\xi_7 \in \mathbf{F}_q$. Consequently, $(s + \sqrt{(s^2 - 4)})/2 \pmod{q}$ can be computed. Now, since $q \equiv 3 \pmod{4}$, then computing a square root of $s^2 - 4$ modulo q reduces to performing the exponentiation modulo q. Let t be the square root of $s^2 - 4 \pmod{q}$, so $t \equiv (s^2 - 4)^{(q+1)/4} \pmod{q}$. Hence ξ_7^i or ξ_7^{-i} is equal to $(s - t)/2 \pmod{q}$, and putting $r \equiv (s - t)/2 \pmod{q}$ we obtain $\Phi_7(r) \equiv 0 \pmod{q}$. Finally, suppose that $n = 14$. We have $\Phi_7(x) = \Phi_{14}(-x)$, so $\Phi_{14}(-r) \equiv 0 \pmod{q}$. We have shown that the procedure FindRootModuloQ finds the root r of $\Phi_n(x)$ modulo q. Now, let us assume that the procedure FindPrimeQ returns a prime $p \equiv r \pmod{q}$. Hence $\Phi_n(p) \equiv \Phi_n(r) \pmod{q}$ and so $q | \Phi_n(p)$. This finishes the proof. $\square$

5. Conclusions

Let a, b, c be the integers such that $q = |N(a + b\eta_1 + c\eta_2)| \equiv 15 \pmod{28}$ is a prime. In this paper we have introduced a deterministic algorithm for computing primitive 7th and 14th roots of unity in $\mathbf{F}_q$ using $O((\log q)^3)$ bit operations. Given such a root of unity and q we can easily find a prime p such that q divides $\Phi_7(p)$ or $\Phi_{14}(p)$. Such primes are key parameters for the cryptosystem based on 7th or 14th order characteristic sequences.

References

[1] Lenstra A. K., Verhuel E. R., The XTR Public Key System, Proceedings of Crypto 2000, LNCS 1880, Springer-Verlag (2000): 1.

[2] Gong G., Harn L., Public-Key Cryptosystems Based on Cubic Finite Field Extension, IEEE IT, 45(7) (1999): 2601.

[3] Gong G., Harn L., A New Approach on Public–key Distribution, ChinaCRYPT (1998): 50.

[4] Giuliani K., Gong G., Analogues to the Gong–Harn and XTR Cryptosystem, Combinatorics and Optimization Research Report CORR 2003–34, University of Waterloo (2003).

[5] Giuliani K., Gong G., New LFSR-Based Cryptosystems and the Trace Discrete Log Problem (Trace-DLP), In: Sequence and Their Applications, SETA 2004. LNCS 3486, Springer-Verlag (2005): 298.

[6] Cox D. A., Primes of the forms $x^2 + ny^2$, Wiley, New York (1989).