Multiplicative orders of elements in Conway’s towers of finite fields

Roman Popovych

Department of Computer Technologies, Lviv Polytechnic National University, Bandery Str. 12, Lviv 79013, Ukraine

e-mail: rombp07@gmail.com

Abstract. We give a lower bound on multiplicative orders of some elements in defined by Conway towers of finite fields of characteristic two and also formulate a condition under that these elements are primitive.

Classification code: AMS 11T30

Keywords: finite field; multiplicative order, Conway’s tower

Elements with high multiplicative order are often needed in several applications that use finite fields [11]. Ideally we want to have a possibility to obtain a primitive element for any finite field. However, if we have no the factorization of the order of finite field multiplicative group, it is not known how to rich the goal. That is why one considers less ambitious question: to find an element with provable high order. It is sufficient in this case to obtain a lower bound on the order. The problem is considered both for general and special finite fields [1,3,7,12,13].

Another less ambitious, but supposedly more important question is to find primitive elements for a class of special finite fields. A polynomial algorithm that find a primitive element in finite field of small characteristic is described in [8]. However, the algorithm relies on two unproved assumptions and is not supported by any computational example. Our paper can be considered as a step towards this direction. We give a lower bound on multiplicative order of some elements in binary recursive extensions of finite fields defined by Conway [4,5,14] and also formulate a condition under that these elements are primitive. \(F_q\) denotes finite field with \(q\) elements. More precisely, we consider the following finite fields:

\[c_{-1} = 1, \quad L_{-1} = F_2(c_{-1}) = F_2;\]

for \(i \geq -1\), \(L_{i+1} = L_i(c_{i+1})\), where \(c_{i+1}\) satisfies the equation \(c_{i+1}^2 + c_{i+1} + \prod_{j=-1}^{i} c_j = 0\).

So, the following tower of finite fields of characteristic two arises:

\[L_{-1} = F_2(c_{-1}) = F_2 \subset L_0 = F_2(c_0) \subset L_1 = L_0(c_1) \subset L_2 = L_4(c_2) \subset ...\]

Such construction is very attractive from point of view of applications, since one can perform operations with finite field elements recursively, and therefore effectively [9].

It is easy to verify directly the following facts: element \(c_0\) is primitive in \(L_0\), and element \(c_1\) is primitive in \(L_1\). On the other hand, H. Lenstra [10, exercise 2] showed: if \(i \geq 2\), then element \(c_i\) is not primitive in \(L_i\). Some primitive elements for the fields \(L_2, L_3, L_4\) are found in [2]. Therefore, for \(i \geq 2\), the following questions arise: 1) give a lower bound on the multiplicative order \(O(c_i)\) of element \(c_i\); 2) what elements are primitive in the fields \(K_i\). We answer partially the questions in theorems 3, 4 and corollaries 2, 3, 4, 5.

Date: 07 September 2015
1. Preliminaries

Point out that, for \( i \geq 0 \), the number of elements of the multiplicative group \( L_i^* = L_i \setminus \{0\} \) equals to \( 2^{2^{i+1}} - 1 \). If to denote the Fermat numbers \( N_j = 2^{2^j} + 1 \ (j \geq 0) \), then the cardinality of \( L_i^* \) equals to \( \prod_{j=0}^{i} N_j \). We use for \( k \geq 0 \) the denotation \( a_k = \prod_{j=0}^{k} c_j \). \( (a,b) \) denotes the greatest common divisor of the numbers \( a \) and \( b \). \( a \mid b \) means that \( a \) divides \( b \).

**Lemma 1** [6, section 1.3]. For \( i \geq 1 \), \( N_i = \prod_{j=0}^{i-1} N_j + 2 \).

**Lemma 2** [6, section 1.3]. Any two Fermat numbers are coprime.

**Lemma 3.** For \( j \geq 2 \), a divisor \( \alpha > 1 \) of the number \( N_j \) is of the form \( \alpha = l \cdot 2^{j+2} + 1 \), where \( l \) is a positive integer.

**Proof.** The result obtained by Euler and Lucas (see [6, theorem 1.3.5]) states: for \( j \geq 2 \), a prime divisor of the number \( N_j \) is of the form \( l \cdot 2^{j+2} + 1 \), where \( l \) is a positive integer. Clearly a product of two numbers of the specified form is a number of the same form. Hence, the result follows. \( \square \)

**Lemma 4.** For \( i \geq 2 \), \( (N_i + 1, N_j) = 1 \) for \( 1 \leq j \leq i - 1 \).

**Proof.** According to lemma 1, \( N_i + 1 = \prod_{j=0}^{i-1} N_j + 3 \). Common divisor of numbers \( N_i + 1 \) and \( \prod_{j=0}^{i-1} N_j \) divides their difference that equals to 3. As \( N_0 = 3 \), we have \( (N_i + 1, \prod_{j=0}^{i-1} N_j) = 3 \). Since, according to lemma 2, numbers \( N_j \) are coprime, \( (N_i + 1, N_j) = 1 \) for \( i \geq 2 \) and \( 1 \leq j \leq i - 1 \). \( \square \)

**Lemma 5.** For \( i \geq 1 \), the equalities
\[
(c_i)^{N_i} = a_{i-1} \tag{1}
\]
and
\[
(a_i)^{N_i} = (a_{i-1})^{N_i+1} \tag{2}
\]
are true.

**Proof.** Show first that (1) holds. Indeed, note that \( c_i \) is a root of the equation \( x^2 + x + a_{i-1} = 0 \) over the field \( L_{i-1} \). One can verify directly, that \( c_i + 1 \) is also a root of this equation. Then \( c_i \) and \( c_i + 1 \) are conjugates [11] over \( L_{i-1} = F_{2^{2^i}} \), that is \( (c_i)_{2^{2^i}} = c_i + 1 \). Therefore, \( (c_i)_{2^{2^{i+1}}} = (c_i + 1)c_i = a_{i-1} \), and the equality (1) is true. Applying (1), we obtain \( (a_i)^{N_i} = (c_i a_{i-1})^{N_i} = (a_{i-1})^{N_i+1} \). Hence, (2) is true as well. \( \square \)
If \( u_j \) is a sequence of integers and \( s > t \), then we consider below the empty product
\[
\prod_{j=1}^{t} u_j = 1.
\]

**Lemma 6.** For \( k \geq 0 \), the following equalities are true
\[
(c_i)^{N_{i-j}} = (a_{i-k-1})^{N_{i-k}}
\]
and
\[
(a_i)^{N_{i-j}} = (a_{i-k-1})^{N_{i-k}}
\]
for \( i > k \).

**Proof.** We will prove this by induction on \( k \). For \( k = 0 \) (and for \( i \geq 1 \)) we have the equalities (1) and (2).

Assume the equalities (3) and (4) hold for \( k - 1 \), that is
\[
(c_i)^{N_{i-j}} = (a_{i-(k-1)-1})^{N_{i-(k-1)}}
\]
and
\[
(a_i)^{N_{i-j}} = (a_{i-(k-1)-1})^{N_{i-(k-1)}}.
\]
Show first that (3) is also true for \( k \). Indeed, applying (5) and (2), we obtain
\[
(c_i)^{N_{i-j}} = \left( (c_i)^{N_{i-j}} \right)^{N_{i-k}} = (a_{i-k-1})^{N_{i-k}}.
\]
Show now that (4) is also true for \( k \). Really, applying (6) and (2), we obtain
\[
(a_i)^{N_{i-j}} = \left( (a_i)^{N_{i-j}} \right)^{N_{i-k}} = (a_{i-k-1})^{N_{i-k}}.
\]

**Lemma 7.** Let \( K \subset L \) be a tower of fields. Let \( x \in L \setminus K \) and \( m \) be the smallest positive integer, satisfying the condition \( x^m \in K \). If \( x^n \in K \) for a positive integer \( n \), then \( m \mid n \).

**Proof.** One can write \( n = um + v \), where \( 0 \leq v < m \). Then \( x^n = (x^m)^u \cdot x^v \), and, therefore, \( x^v \in K \). As \( m \) is the smallest positive integer with the condition \( x^m \in K \) and \( v < m \), we have \( v = 0 \), and the result follows.

**Lemma 8.** For \( u \geq 1 \), if \( (c_u)^l \in L_{u-l} \), where \( l \) is a positive integer, then \( (l, N_u) > 1 \).

**Proof.** The equality (1) gives \( (c_u)^N = a_{u-1} \in L_{u-1} \). According to lemma 7, if \( d \) is the smallest positive integer with \( (c_u)^d \in L_{u-1} \), then \( d \mid N_u \) and \( d \mid l \). Clearly \( d > 1 \). Therefore \( (l, N_u) \geq d > 1 \).
Lemma 9. Let \( L_0 \subset L_2 \) be a tower of fields and \( b \in L_2^* \). Let \( b^r = a \in L_2^* \) and \( r \) be the smallest positive integer with \( b^r \in L_2^* \). Then \( O(b) = r \cdot O(a) \).

Proof. As \( b^{O(b)} = 1 \in L_2^* \), one has \( O(b) \geq r \). Write \( O(b) = s \cdot r + t \), where \( s \in \mathbb{N} \) and \( 0 \leq t < r \). Then
\[
1 = b^{O(b)} = b^{s \cdot r + t} = a^t b^r.
\]
Hence, \( b^r = a^t \in L_2^* \). By definition of \( r \), it is possible only for \( t = 0 \). We have \( a^s = 1 \), \( s \geq O(a) \) and \( O(b) = s \cdot r \cdot O(a) \). From the other side, \( b^{O(a)} = a^{O(a)} = 1 \), and therefore \( O(b) = r \cdot O(a) \). ∎

Theorem 1. For \( i \geq 2 \), \( (c_i)_{j=0}^{N_{i-j}} \in L_{r-i} \setminus L_{r-2} \) for \( 0 \leq k \leq i - 1 \).

Proof. Applying equality (3), one obtains
\[
(c_i)_{j=0}^{N_{i-j}} \prod_{j=0}^{k}(a_{j-k})_j = (c_{i-k-1})_{j=0}^{N_{i-j+1}} \prod_{j=0}^{k}(a_{j-k-2})_j = (c_{i-k-1})_{j=0}^{N_{i-j+1}} (a_{j-k-2})_j = (7).
\]
Obviously \( (c_{i-k-1})_{j=0}^{N_{i-j+1}} \in L_{r-i} \) and \( (a_{j-k-2})_j \in L_{r-i} \). Hence, the product on the right hand of equality (7) belongs to \( L_{r-i} \). For \( 1 \leq j \leq k \), according to lemma 4, \( (N_{i-j} + 1, N_{i-k-1}) = 1 \) and
\[
\prod_{j=0}^{k}(N_{i-j} + 1, N_{i-k-1}) = 1.
\]
Then, by lemma 8, \( (c_{i-k-1})_{j=0}^{N_{i-j+1}} \prod_{j=0}^{k}(N_{i-j+1}) \notin L_{r-i} \). Therefore, the element
\[
(c_{i-k-1})_{j=0}^{N_{i-j+1}} (a_{j-k-2})_j = \prod_{j=0}^{k}(N_{i-j} + 1, N_{i-k-1})
\]
does not belong to \( L_{r-i} \). ∎

Theorem 2. For \( i \geq 2 \), \( (a_i)_{j=0}^{N_{i-j}} \in L_{r-i} \setminus L_{r-2} \) for \( 0 \leq k \leq i - 1 \).

Proof. Applying equality (4), we have
\[
(a_i)_{j=0}^{N_{i-j}} \prod_{j=0}^{k}(a_{j-k})_j = (c_{i-k-1})_{j=0}^{N_{i-j+1}} (a_{j-k-2})_j = (8).
\]
Obviously \( (c_{i-k-1})_{j=0}^{N_{i-j+1}} \in L_{r-i} \) and \( (a_{j-k-2})_j \in L_{r-i} \). Hence, the product on the right hand of the equality (8) belongs to \( L_{r-i} \). For \( 0 \leq j \leq k \), according to lemma 4, \( (N_{i-j} + 1, N_{i-k-1}) = 1 \) and
\[
\prod_{j=0}^{k}(N_{i-j} + 1, N_{i-k-1}) = 1.
\]
So, by lemma 8, \( (c_{i-k-1})_{j=0}^{N_{i-j+1}} \prod_{j=0}^{k}(N_{i-j+1}) \notin L_{r-i} \). Hence, the element
\[
(c_{i-k-1})_{j=0}^{N_{i-j+1}} (a_{j-k-2})_j = \prod_{j=0}^{k}(N_{i-j} + 1, N_{i-k-1})
\]
does not belong to \( L_{r-i} \). ∎
2. Lower bound on multiplicative orders of elements

We give in this section in corollary 2 a lower bound on multiplicative order of elements \( c_i, a_i \) and also formulate in corollary 3 a condition under that these elements are primitive.

**Theorem 3.** For \( i \geq 2 \), the following statements hold:

(a) \( O(c_i) = \prod_{j=1}^{i} \alpha_j \), where \( \alpha_j \mid N_j \), \( \alpha_j > 1 \);

(b) \( O(a_i) = \prod_{j=1}^{i} \beta_j \), where \( \beta_j \mid N_j \), \( \beta_j > 1 \).

**Proof.** (a) Define recursively the sequence \( \alpha_1, \ldots, \alpha_i \) of positive integers as follows. \( \alpha_i \) is the smallest integer satisfying the condition \((c_i)^{\alpha_i} \in L_{i-1}\). If \( \alpha_1, \ldots, \alpha_{i-1} \), where \( 0 \leq j \leq i-2 \), are already known, then \( \alpha_{i-1} \) is the smallest positive integer such that the condition

\[
\prod_{j=1}^{i} \alpha_j^{\alpha_{i-1}} \in L_{i-2}
\]

holds.

Since the cardinality of the group \( L_i \) equals to \( \prod_{j=0}^{i} N_j \) and the cardinality of the group \( L_{i-1} \) equals to \( \prod_{j=0}^{i-1} N_j \), we have that the number of elements of the factor-group \( L_i / L_{i-1} \) equals to \( N_i \). If \( d \) is the coset of \( c_i \) in the factor-group, then \( \alpha_i = O(d) \) and as a consequence of Lagrange’s theorem for finite groups \( \alpha_i \mid N_i \). Clearly, \( \alpha_i > 1 \). \((c_i)^{\alpha_i} \in L_{i-1} \setminus L_{i-2} \), because according to theorem 2 \((c_i)^{N_i} \in L_{i-1} \setminus L_{i-2} \). Indeed, if to suppose \((c_i)^{\alpha_i} \in L_{i-2} \), then \( [(c_i)^{\alpha_i}]^{N_i/N_j} = (c_i)^{N_i} \in L_{i-2} \) - a contradiction. According to lemma 9, \( O(c_i) = \alpha_i O((c_i)^{\alpha_i}) \).

Analogously to the previous, one can show in the case of finding \( \alpha_{i-1} \) that \( \alpha_{i-1} \mid N_{i-1} \)

\((\alpha_{i-1} > 1) \) and \( \prod_{j=1}^{i} \alpha_j^{\alpha_{i-1}} \in L_{i-2} \setminus L_{i-3} \). According to lemma 9, \( O((c_i)^{\alpha_{i-1}}) = \alpha_{i-1} O((c_i)^{\alpha_{i-1}}) \).

Since, according to (3),

\[ (c_i)^{N_i} = (\alpha_0^{N_i+1})^{\prod_{j=0}^{i} (N_i+1)} = 1, \]

one obtains \( O(c_i) \prod_{j=0}^{i-1} N_{i-j} \), and \( O(c_i) = \alpha_1 \ldots \alpha_i \).

(b) The proof is analogous to the previous one, using theorem 2 instead of theorem 1.

\[ \square \]
Corollary 1. For $i \geq 2$, $O(c_i c_0) = N_0 O(c_i)$ and $O(a_i a_0) = N_0 O(a_i)$.

Proof. Note that $O(c_0) = N_0$. Since, according to theorem 3, $O(c_i)$ divides $\prod_{j=1}^{i} N_j$, and lemma 2 gives $(\prod_{j=1}^{i} N_j, N_0) = 1$, we have $(O(c_i), O(c_0)) = 1$. Then $O(c_i c_0) = O(c_i) O(c_0)$, and the result for $c_i c_0$ follows. The proof for $a_i a_0 = a_i c_0$ is analogous.

Corollary 2. The multiplicative order of the element $c_i$ and the element $a_i$ equals to $\prod_{j=1}^{i} N_j$ for $2 \leq i \leq 4$ and is at least $\prod_{j=1}^{i} N_j \cdot \prod_{j=5}^{i} (2^{j+2}+1)$ for $i \geq 5$.

Proof. Consider the formulas for the multiplicative order of $c_i$ and $a_i$ given in theorem 3. It is known that for $1 \leq j \leq 4$ the Fermat numbers $N_1 = 5$, $N_2 = 17$, $N_3 = 257$, $N_4 = 65537$ are prime [6, table 1.3]. Therefore, $\alpha_j = \beta_j = N_j$ for $1 \leq j \leq 4$. According to lemma 3, for $j \geq 5$, $\alpha_j \beta_j \geq 2^{j+2}+1$.

Theorem 4. Let $i \geq 5$. For $5 \leq i \leq 4$, if $\alpha_j = N_j$ is the smallest positive integer satisfying the condition $(c_j)^{\alpha_j} \in L_{j-1}$, then $O(a_i) = O(c_i) = \prod_{j=1}^{i} N_j$.

Proof. For element $a_i$, the proof is by induction on $i \geq 5$. Note that $\alpha_j$ is the smallest positive integer with $(c_j)^{\alpha_j} \in L_{j-1}$ iff $\alpha_j$ is the smallest positive integer with $(a_j)^{\alpha_j} \in L_{j-1}$.

For $i = 5$ we have from equality (2) $(a_5)^{N_5} = (a_5)^{N_5+1}$. Then, according to lemma 9, $O(a_5) = N_5 O((a_5)^{N_5+1})$. We have $O(a_4) = \prod_{j=1}^{4} N_j$ by corollary 2 and $(N_5 + 1, \prod_{j=1}^{4} N_j) = 1$ by lemma 4. Now use the well known fact that raising an element of a group to a power relatively prime to its order does not change the order. One obtains $O((a_4)^{N_5+1}) = O(a_4)$ and $O(a_5) = \prod_{j=1}^{5} N_j$.

Assume the statement of the theorem is true for $i - 1$. For $i$ we have from equality (2) $(a_i)^{N_i} = (a_{i-1})^{N_i+1}$. Then, according to lemma 9, $O(a_i) = N_i O((a_{i-1})^{N_i+1})$. As $O(a_{i-1}) = \prod_{j=1}^{i-1} N_j$ by induction assumption and $(N_i + 1, \prod_{j=1}^{i-1} N_j) = 1$ by lemma 4, one has, analogously to the previous, $O((a_{i-1})^{N_i+1}) = O(a_{i-1})$ and $O(a_i) = \prod_{j=1}^{i} N_j$. 

To complete the proof note that, according to equality (1) and lemma 9, $O(c_i) = N_i O(a_{i-1}) = O(a_i)$.

Remark that, if the condition of theorem 4 is true, then one has the following chain of cyclic subgroups:

$$\{c_i\} = \{a_i\} \supset \{c_{i-1}\} = \{a_{i-1}\} \supset \ldots \supset \{c_2\} = \{a_2\} \supset \{a_1\}.$$ 

At the same time $\{a_i\} \neq \{c_i\}$, because $O(c_i) = 15$, $O(a_i) = O(c_i a_i) = 5$.

As a consequence of theorem 4 and corollary 1, one has the following corollary.

**Corollary 3.** Let $i \geq 5$. For $5 \leq j \leq i$, if $\alpha_j = N_j$ is the smallest positive integer with $(c_j)^{\alpha_j} \in L_{i-1}$, then $c_j c_0$ and $a_j a_0$ is primitive.

**Proof.** Since $O(c_i c_0) = O(a_i a_0) = \prod_{j=0}^{i} N_j$, the result follows.

**Theorem 5.** For $5 \leq j \leq 11$, the number $\alpha_j = N_j$ is the smallest positive integer with $(c_j)^{\alpha_j} \in L_{j-1}$.

**Proof.** For $5 \leq j \leq 11$, the Fermat numbers are completely factored into primes [6]. Correspondent factorizations and connected with them results of verification are given below. Note that to prove the fact: $N_j$ is the smallest positive integer with $(c_j)^{\alpha_j} \in L_{j-1}$, it is enough to verify $c_j^{N_j/p} \notin L_{j-1}$ for any prime divisor $p$ of $N_j$. Really, if element $c_j$ in the power $N_j/p$ does not belong to $L_{j-1}$, then element $c_j$ in the power of any divisor $N_j/(pq)$ of $N_j/p$ does not belong to $L_{j-1}$ as well.

For $j = 5$, one has the factorization $N_5 = 641 \cdot 6700417$. According to equality (1), $(c_5)^{N_5} = c_2 c_3 c_2 c_0 \in L_4$. We have verified that $\alpha_5 = N_5$ is the smallest positive integer with $(c_5)^{\alpha_5} \in L_4$.

For $j = 6$, one has the factorization $N_6 = 274177 \cdot 67280421310721$. According to equality (1), $(c_6)^{N_6} = c_3 c_6 c_5 c_2 c_1 c_0 \in L_5$. We have verified that $\alpha_6 = N_6$ is the smallest positive integer with $(c_6)^{\alpha_6} \in L_5$.

For $j = 7$ one has the factorization $N_7 = 59649589127497217 \cdot 5704689200685129054721$. According to equality (1), $(c_7)^{N_7} = c_5 c_6 c_5 c_4 c_3 c_2 c_1 c_0 \in L_6$. We have verified that $\alpha_7 = N_7$ is the smallest positive integer with $(c_7)^{\alpha_7} \in L_6$.

For $j = 8$, one has the factorization $N_8 = 1238926361552897 \cdot P_{62}$, where $P_{62}$ is a prime with 62 decimal digits, $P_{62} = 93461369715357977769163558199606896584051237541638188580280321$. According to equality (1), $(c_8)^{N_8} = c_7 c_6 c_5 c_6 c_5 c_4 c_3 c_2 c_1 c_0 \in L_7$. We have verified that $\alpha_8 = N_8$ is the smallest positive integer with $(c_8)^{\alpha_8} \in L_7$.

For $j = 9$, one has the factorization $N_9 = 2424833 \cdot 7455602825647884208337395736200454918783366342657 \cdot P_{99}$, where $P_{99}$ is a prime number with 99 decimal digits,
According to equality (1), \((c_g)^N = c_g c_6 c_5 c_4 c_3 c_2 c_1 c_0 \in L_g\). We have verified that \(\alpha_g = N_g\) is the smallest positive integer with \((c_g)^{\alpha_g} \in L_g\).

For \(j = 10\), one has the factorization
\[
N_{10} = 45592577 \cdot 6487031809 \cdot 4659775785220018543264560743076778192897 \cdot P_{252},
\]
where \(P_{252}\) is a prime with 252 decimal digits,
\[
P_{252} = 130439874405488189727484768796509939466085308416118921686952957768324162514
7186357414022797757310489589783928842923844831149032913798729088601617946094119
44901059590671013053190617101835449160961919391248853811608071229967232280621782
0753127014424577.
\]
According to equality (1), \((c_{10})^N = c_{10} c_9 c_8 c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0 \in L_g\). We have verified that \(\alpha_{10} = N_{10}\) is the smallest positive integer with \((c_{10})^{\alpha_{10}} \in L_g\).

For \(j = 11\), one has the factorization
\[
N_{11} = 319489 \cdot 974849 \cdot 167988556341760471537 \cdot 3560841906445833920513 \cdot P_{564},
\]
where \(P_{564}\) is a prime with 564 decimal digits,
\[
P_{564} = 17346244717914755543025897086430977837774218447236640846493470190613635791928
7910885791038330408837177983810868451546421940712978306134189864280826014542758
708589243873685536397311894886939915854550661114742021613255701726056413939436694
579332296866510895968548207053880726458285541519364019124649311825460928798157330
5779557335850498227928009042872567591518912118622751714319229788100979251036035
4969172799112663523587832366471931547770914277453770382945849189175903251109398
1322486044298573971650711059244462177542540706913047034664436034913824417233065
98834177.
\]
According to equality (1), \((c_{11})^N = c_{11} c_9 c_8 c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0 \in L_g\). We have verified that \(\alpha_{11} = N_{11}\) is the smallest positive integer with \((c_{11})^{\alpha_{11}} \in L_g\).

**Corollary 4.** For \(2 \leq i \leq 11\), the multiplicative order of element \(c_i\) and element \(a_i\) equals to \(\prod_{j=1}^{i} N_j\).

**Proof.** The case \(2 \leq i \leq 4\) follows from corollary 2. The case \(5 \leq i \leq 11\) follows from theorem 4 and theorem 5.

As a consequence of corollary 1 and corollary 4, one has the following corollary.

**Corollary 5.** For \(2 \leq i \leq 11\), the element \(c_i c_0\) and the element \(a_i a_0\) is primitive.
References

1. O. Ahmadi, I.E. Shparlinski, J.F. Voloch, Multiplicative order of Gauss periods, Intern. J. Number Theory 6 (4) (2010) 877-882.
2. L. le Bruyn, , 2010,
   http://www.neverendingbooks.org/the-odd-knights-of-the-round-table
   http://www.neverendingbooks.org/seating-the-first-few-thousand-knights
   http://www.neverendingbooks.org/seating-the-first-few-billion-knights
3. Q. Cheng, On the construction of finite field elements of large order, Finite fields and Their Appl. 11 (3) (2005) 358-366.
4. J.H. Conway, On Numbers and Games, Academic Press, New York, 1976.
5. J.H. Conway, N.J.A. Sloane, Lexicographic codes: error-correcting codes from game theory, IEEE Trans. Inform. theory, 32 (3) (1986) 337-348.
6. R. Crandall, C. Pomerance, Prime Numbers: A Computational Perspective, Springer-Verlag, New York, 2005.
7. S. Gao, Elements of provable high orders in finite fields, Proc. Amer. Math. Soc. 107 (6) (1999) 1615-1623.
8. M.-D. Huang, A.K. Narayanan, Finding primitive elements in finite fields of small characteristic, 2013, http://arxiv.org/abs/1304.1206.
9. H. Ito, T. Kajiwara, H. Song, A Tower of Artin-Schreier extensions of finite fields and its applications, JP J. Algebra, Number Theory Appl. 22 (2) (2011) 111-125.
10. H.W.Lenstra, Nim multiplication, 1978, https://openaccess.leidenuniv.nl/handle/1887/2125.
11. R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, 1997.
12. R. Popovych, Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$, Finite Fields Appl. 18 (4) (2012) 700-710.
13. R. Popovych, Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$, Finite Fields Appl. 19 (1) (2013) 86-92.
14. D.Wiedemann, An iterated quadratic extension of $GF(2)$, Fibonacci Quart. 26 (4) (1988) 290-295.