Algebra and Discrete Mathematics
Volume **25** (2018). Number 1, pp. 137–146

RESEARCH ARTICLE

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

Roman Popovych

Communicated by A. P. Petravchuk

Abstract. We give a lower bound on multiplicative orders of certain elements in defined by Conway towers of finite fields of characteristic 2 and also formulate a condition under that these elements are primitive.

Introduction

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 not any 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 a 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 orders of certain elements in binary recursive

2010 MSC: 11T30.
Key words and phrases: finite field, multiplicative order, Conway's tower.

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.

The following finite fields of characteristic 2 are considered:

$$c_{-1} = 1, L_{-1} = F_2(c_{-1}) = F_2,$$

for $i \geqslant -1$, $L_{i+1} = L_i(c_{i+1})$, 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 arises:

$$L_{-1} = F_2(c_{-1}) = F_2 \subset L_0 = F_2(c_0) \subset L_1 = L_0(c_1) \subset L_2 = L_1(c_2) \subset \ldots$$

Such a construction is very attractive from the 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 $i \geqslant 2$, 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] using SageMath. Therefore, for $i \geqslant 2$, the following questions arise: 1) what is a lower bound on the multiplicative order $O(c_i)$ of element c_i; 2) what elements are primitive in the fields L_i. We partially answer the questions in Theorems 3, 4 and Corollaries 2, 3, 4, 5.

1. Preliminaries

Observe that, for $i \geqslant 0$, the number of elements of the multiplicative group $L_i^* = L_i \backslash \{0\}$ equals $2^{2^{i+1}} - 1$. If to denote the Fermat numbers by $N_j = 2^{2^j} + 1$ $(j \geqslant 0)$, then the cardinality of L_i^* is $\prod_{j=0}^{i} N_j$. We will use for $k \geqslant 0$ the denotation $a_k = \prod_{j=0}^{k} c_j$.

Lemma 1 ([6, Section 1.3.2]). *For $i \geqslant 1$, $N_i = \prod_{j=0}^{i-1} N_j + 2$.*

Lemma 2 ([6, Section 1.3.2]). *Any two Fermat numbers are coprime.*

Lemma 3. *For $j \geqslant 2$, 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 $j \geqslant 2$, a prime divisor of 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. □

Lemma 4. *For $i \geqslant 2$ and $1 \leqslant j \leqslant i-1$, $\gcd(N_i + 1, N_j) = 1$.*

Proof. By lemma 1, $N_i + 1 = \prod_{j=0}^{i-1} N_j + 3$. A common divisor of numbers $N_i + 1$ and $\prod_{j=0}^{i-1} N_j$ divides their difference that equals 3. As $N_0 = 3$, $\gcd(N_i + 1, \prod_{j=0}^{i-1} N_j) = 3$. Since, by lemma 2, numbers N_j are coprime, $\gcd(N_i + 1, N_j) = 1$ for $i \geqslant 2$ and $1 \leqslant j \leqslant i-1$. □

Lemma 5. *For $i \geqslant 1$, the equations*

$$(c_i)^{N_i} = a_{i-1} \tag{1}$$

and

$$(a_i)^{N_i} = (a_{i-1})^{N_i+1}. \tag{2}$$

are true.

Proof. First show that (1) holds. Indeed, note that c_i is a root of 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 (1) is true. Applying (1) shows that $(a_i)^{N_i} = (c_i a_{i-1})^{N_i} = (a_{i-1})^{N_i+1}$. Hence, (2) is true as well. □

If u_j is a sequence of integers and $s > t$, then we will consider below the empty product $\prod_{j=s}^{t} u_j = 1$.

Lemma 6. *For $k \geqslant 0$ and $i > k$, the following equations are true:*

$$(c_i)^{\prod_{j=0}^{k} N_{i-j}} = (a_{i-k-1})^{\prod_{j=1}^{k}(N_{i-j}+1)} \tag{3}$$

and

$$(a_i)^{\prod_{j=0}^{k} N_{i-j}} = (a_{i-k-1})^{\prod_{j=0}^{k}(N_{i-j}+1)} \tag{4}$$

Proof. We will proceed by induction on k. For $k = 0$ (and for $i \geqslant 1$), (3) and (4) coincide with (1) and (2) respectively.

Now, suppose that (3) and (4) hold for $k-1$, namely

$$(c_i)^{\prod_{j=0}^{k-1} N_{i-j}} = (a_{i-(k-1)-1})^{\prod_{j=1}^{k-1}(N_{i-j}+1)} \tag{5}$$

and

$$(a_i)^{\prod_{j=0}^{k-1} N_{i-j}} = (a_{i-(k-1)-1})^{\prod_{j=0}^{k-1}(N_{i-j}+1)}. \tag{6}$$

Then, applying (5) and (2), we obtain

$$(c_i)^{\prod_{j=0}^{k} N_{i-j}} = \Big((c_i)^{\prod_{j=0}^{k-1} N_{i-j}}\Big)^{N_{i-k}} = \big((a_{i-k})^{N_{i-k}}\big)^{\prod_{j=1}^{k-1}(N_{i-j}+1)}$$
$$= (a_{i-k-1})^{\prod_{j=1}^{k}(N_{i-j}+1)}.$$

Hence, (3) is true for k. Analogously, exploiting (6) and (2) shows that

$$(a_i)^{\prod_{j=0}^{k} N_{i-k}} = \Big((a_i)^{\prod_{j=0}^{k-1} N_{i-k}}\Big)^{N_{i-k}} = \big((a_{i-k})^{N_{i-k}}\big)^{\prod_{j=0}^{k-1}(N_{i-j}+1)}$$
$$= (a_{i-k-1})^{\prod_{j=0}^{k}(N_{i-j}+1)},$$

and (4) is true for k as well. This completes the induction and the proof. □

Lemma 7. *Let $K \subset L$ be a tower of fields. Let $x \in L\backslash K$ 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 $m|n$.*

Proof. One may write $n = um+v$, where $0 \leqslant v < m$. 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. *Let $u \geqslant 1$ and l be a positive integer. If $(c_u)^l \in L_{u-1}$, then $(l, N_u) > 1$.*

Proof. (1) implies that $(c_u)^{N_u} = a_{u-1} \in L_{u-1}$. By Lemma 7, if d is the smallest positive integer with $(c_u)^d \in L_{u-1}$, then $d|N_u$ and $d|l$. Clearly, $d > 1$, and hence, $(l, N_u) \geqslant d > 1$. □

Lemma 9. *Let $L_1 \subset L_2$ be a tower of fields and $b \in L_2^*$. Let $b^r = a \in L_1^*$ and r be the smallest positive integer with $b^r \in L_1^*$. Then $O(b) = r \cdot O(a)$.*

Proof. Since $b^{O(b)} = 1 \in L_1^*$, the inequality $O(b) \geqslant r$ holds. Write $O(b) = sr + t$, where s is a positive integer and $0 \leqslant t < r$. Then

$$1 = b^{O(b)} = b^{sr+t} = a^s b^t.$$

Hence, $b^t = a^{-s} \in L_1^*$. By definition of r, it is possible only for $t = 0$. Therefore, $a^s = 1$, $s \geqslant O(a)$ and $O(b) = sr \geqslant r \cdot O(a)$. From the other side, $b^{r \cdot O(a)} = a^{O(a)} = 1$, and thus $O(b) = r \cdot O(a)$. □

Theorem 1. *The relation* $(c_i)^{\prod_{j=0}^{k} N_{i-j}} \in L_{i-k-1} \backslash L_{i-k-2}$ *holds for* $i \geqslant 2$ *and* $0 \leqslant k \leqslant i-1$.

Proof. Applying (3), we see that

$$(c_i)^{\prod_{j=0}^{k} N_{i-j}} = (c_{i-k-1})^{\prod_{j=1}^{k}(N_{i-j}+1)} (a_{i-k-2})^{\prod_{j=1}^{k}(N_{i-j}+1)}. \qquad (7)$$

Obviously, $(c_{i-k-1})^{\prod_{j=1}^{k}(N_{i-j}+1)} \in L_{i-k-1}$ and $(a_{i-k-2})^{\prod_{j=1}^{k}(N_{i-j}+1)} \in L_{i-k-2}$. Hence, the product on the right hand of (7) belongs to L_{i-k-1}. For $1 \leqslant j \leqslant k$, by Lemma 4, $\gcd(N_{i-j}+1, N_{i-k-1}) = 1$, and thus $\gcd(\prod_{j=1}^{k}(N_{i-j}+1), N_{i-k-1}) = 1$. Then, by Lemma 8, the relation $(c_{i-k-1})^{\prod_{j=1}^{k}(N_{i-j}+1)} \notin L_{i-k-2}$ is true. Therefore, the element

$$(c_{i-k-1})^{\prod_{j=1}^{k}(N_{i-j}+1)} (a_{i-k-2})^{\prod_{j=1}^{k}(N_{i-j}+1)}$$

does not belong to L_{i-k-2}. □

Theorem 2. *The relation* $(a_i)^{\prod_{j=0}^{k} N_{i-j}} \in L_{i-k-1} \backslash L_{i-k-2}$ *holds for* $i \geqslant 2$ *and* $0 \leqslant k \leqslant i-1$.

Proof. Using (4), we have

$$(a_i)^{\prod_{j=0}^{k} N_{i-j}} = (c_{i-k-1})^{\prod_{j=0}^{k}(N_{i-j}+1)} (a_{i-k-2})^{\prod_{j=0}^{k}(N_{i-j}+1)}. \qquad (8)$$

Observe that $(c_{i-k-1})^{\prod_{j=0}^{k}(N_{i-j}+1)} \in L_{i-k-1}$ and $(a_{i-k-2})^{\prod_{j=0}^{k}(N_{i-j}+1)} \in L_{i-k-2}$. Thus, the product on the right hand of (8) belongs to L_{i-k-1}. For $0 \leqslant j \leqslant k$, by Lemma 4, $\gcd(N_{i-j}+1, N_{i-k-1}) = 1$, and therefore $\gcd(\prod_{j=0}^{k}(N_{i-j}+1), N_{i-k-1}) = 1$. So, the relation $(c_{i-k-1})^{\prod_{j=0}^{k}(N_{i-j}+1)} \notin L_{i-k-2}$ holds by Lemma 8. Hence, the element

$$(c_{i-k-1})^{\prod_{j=0}^{k}(N_{i-j}+1)} (a_{i-k-2})^{\prod_{j=0}^{k}(N_{i-j}+1)}$$

does not belong to L_{i-k-2}. □

2. Lower bound on multiplicative orders of elements

We give in this section in Corollary 2 a lower bound on multiplicative orders of elements c_i, a_i and also formulate in Corollary 3 a condition under that these elements are primitive.

Theorem 3. *For* $i \geqslant 2$, *the following statements hold:*

(a) $O(c_i) = \prod_{j=1}^{i} \alpha_j$, *where* $\alpha_j | N_j$, $\alpha_j > 1$;
(b) $O(a_i) = \prod_{j=1}^{i} \beta_j$, *where* $\beta_j | N_j$, $\beta_j > 1$.

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

$$\{(c_i)^{\prod_{k=i-j}^{i} \alpha_k}\}^{\alpha_{i-j-1}} \in L_{i-j-2}$$

holds.

Since the cardinality of the group L_i^* is $\prod_{j=0}^{i} N_j$ and the cardinality of the group L_{i-1}^* is $\prod_{j=0}^{i-1} N_j$, we have that the number of elements of the factor-group L_i^*/L_{i-1}^* equals 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, $\alpha_i | N_i$. Clearly, $\alpha_i > 1$. By Theorem 2 $(c_i)^{N_i} \in L_{i-1} \backslash L_{i-2}$, and thus $(c_i)^{\alpha_i} \in L_{i-1} \backslash L_{i-2}$. Indeed, if to suppose that $(c_i)^{\alpha_i} \in L_{i-2}$, then $[(c_i)^{\alpha_i}]^{N_i/\alpha_i} = (c_i)^{N_i} \in L_{i-2}$, a contradiction. Hence, by Lemma 9, $O(c_i) = \alpha_i O((c_i)^{\alpha_i})$.

Analogously, one can show that $\alpha_{i-j-1} | N_{i-j-1}$ $(\alpha_{i-j-1} > 1)$ and $\{(c_i)^{\prod_{k=i-j}^{i} \alpha_{i-k}}\}^{\alpha_{i-j-1}} \in L_{i-j-2} \backslash L_{i-j-3}$. By Lemma 9,

$$O((c_i)^{\alpha_i \ldots \alpha_{i-j}}) = \alpha_{i-j-1} O((c_i)^{\alpha_i \ldots \alpha_{i-j} \alpha_{i-j-1}}).$$

From (3), we deduce that

$$(c_i)^{\prod_{j=0}^{i-1} N_{i-j}} = ((a_0)^{N_1+1})^{\prod_{j=1}^{i-2}(N_{i-j}+1)} = 1.$$

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

(b) The proof is analogues to the previous one, using Theorem 2 instead of Theorem 1. □

Corollary 1. *For* $i \geqslant 2$, $O(c_i c_0) = N_0 O(c_i)$ *and* $O(a_i a_0) = N_0 O(a_i)$.

Proof. Note that $O(c_0) = N_0$. Since, by Theorem 3, $O(c_i)$ divides $\prod_{j=1}^{i} N_j$, and lemma 2 implies that $\gcd(\prod_{j=1}^{i} N_j, N_0) = 1$, we have $\gcd(O(c_i), O(c_0)) = 1$. Therefore, $O(c_i c_0) = O(c_i) O(c_0)$, 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 elements* c_i *and* a_i *equals* $\prod_{j=1}^{i} N_j$ *for* $2 \leqslant i \leqslant 4$ *and is at least* $\prod_{j=1}^{4} N_j \cdot \prod_{j=5}^{i}(2^{j+2}+1)$ *for* $i \geqslant 5$.

Proof. Consider the formulas for the multiplicative order of c_i and a_i given in Theorem 3. For $1 \leqslant j \leqslant 4$ 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 $1 \leqslant j \leqslant 4$. By Lemma 3, $\alpha_j, \beta_j \geqslant 2^{j+2} + 1$ for $j \geqslant 5$. □

Theorem 4. *Let $i \geqslant 5$. If, for $5 \leqslant j \leqslant i$, the $\alpha_j = N_j$ 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. First prove the theorem for element a_i. Note that α_j is the smallest positive integer with $(c_j)^{\alpha_j} \in L_{j-1}$ iff α_j is the smallest positive integer with $(a_j)^{\alpha_j} \in L_{j-1}$. We will proceed by induction on $i \geqslant 5$.

For $i = 5$, we have from (2) that $(a_5)^{N_5} = (a_4)^{N_5+1}$. Thus, by Lemma 9, $O(a_5) = N_5 O((a_4)^{N_5+1})$. We have $O(a_4) = \prod_{j=1}^{4} N_j$ by Corollary 2 and $\gcd(N_5 + 1, \prod_{j=1}^{4} N_j) = 1$ by Lemma 4. 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 deduces that $O((a_4)^{N_5+1}) = O(a_4)$ and $O(a_5) = \prod_{j=1}^{5} N_j$.

Now, assume that the statement of the theorem is true for $i-1$. For i, we have from (2) that $(a_i)^{N_i} = (a_{i-1})^{N_i+1}$. Therefore, by 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 the induction assumption and $\gcd(N_i + 1, \prod_{j=1}^{i-1} N_j) = 1$ by Lemma 4, one obtains, analogously to the previous, that $O((a_{i-1})^{N_i+1}) = O(a_{i-1})$ and $O(a_i) = \prod_{j=1}^{i} N_j$. This completes the induction

To complete the proof, observe that, by 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 the following chain of cyclic subgroups arises:

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

At the same time, $\langle a_1 \rangle \neq \langle c_1 \rangle$, because $O(c_1) = 15$, $O(a_1) = O(c_1 c_0) = 5$.

Theorem 4 and Corollary 1 imply the following corollary.

Corollary 3. *Let $i \geqslant 5$. If, for $5 \leqslant j \leqslant i$, the $\alpha_j = N_j$ is the smallest positive integer with $(c_j)^{\alpha_j} \in L_{j-1}$, then $c_i c_0$ and $a_i a_0$ are 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 $5 \leqslant j \leqslant 11$, the number $\alpha_j = N_j$ is the smallest positive integer with $(c_j)^{\alpha_j} \in L_{j-1}$.*

Proof. 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 $5 \leqslant j \leqslant 11$, the Fermat numbers N_j are completely factored into primes [6]. These factorizations are provided in Appendix. By equation (1), $(c_i)^{N_i} = a_{i-1} \in L_{i-1}$. We have verified for $5 \leqslant j \leqslant 11$, using the factorizations and computer calculations, that $\alpha_j = N_j$ is the smallest positive integer with $(c_j)^{\alpha_j} \in L_{j-1}$. □

Corollary 4. *For* $2 \leqslant i \leqslant 11$*, the multiplicative order of elements* c_i *and* a_i *equals* $\prod_{j=1}^{i} N_j$*.*

Proof. The result in the case $2 \leqslant i \leqslant 4$ follows from Corollary 2. The result in the case $5 \leqslant i \leqslant 11$ follows from Theorem 4 and Theorem 5. □

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

Corollary 5. *For* $2 \leqslant i \leqslant 11$*, the elements* $c_i c_0$ *and* $a_i a_0$ *are primitive.*

Let us consider, for example, the multiplicative group of the field L_2. The multiplicative order of element c_2 is $O(c_2) = 5 \cdot 17 = 85$. Element $c_2 c_0$ is primitive, namely $O(c_2 c_0) = 3 \cdot 5 \cdot 17 = 255$. Since $c_2 + c_1 + 1 = (c_2)^5$, the order of element $c_2 + c_1 + 1$ is $O(c_2 + c_1 + 1) = 17$.

Appendix

$$N_5 = 641 \cdot 6700417,$$
$$N_6 = 274177 \cdot 67280421310721,$$
$$N_7 = 59649589127497217 \cdot 5704689200685129054721,$$
$$N_8 = 1238926361552897 \cdot P_{62},$$

where P_{62} is prime with 62 decimal digits

$$P_{62} = 93461639715357977769163558199606896584051237541638188580\\280321,$$
$$N_9 = 7455602825647884208337395736200454918783366342657\\ \cdot 2424833 \cdot P_{99},$$

where P_{99} is prime with 99 decimal digits

$$\begin{aligned}
P_{99} = {} & 741640062627530801524787141901937474059940781097519023 90\\
& 582131614441575950470500809281871169394073 7,
\end{aligned}$$

$$\begin{aligned}
N_{10} = {} & 45592577 \cdot 6487031809\\
& \cdot 46597757852200185432645607430767781928 97 \cdot P_{252},
\end{aligned}$$

where P_{252} is prime with 252 decimal digits

$$\begin{aligned}
P_{252} = {} & 13043987440548818972748476879650990394660853084161189 21\\
& 86895295776832416251471863574140227977573104895898783 92\\
& 88429238448311490329137987290886016179460941194490105 95\\
& 90671013053190617101835449160961919391248853811608071 22\\
& 996723228062178207531270144245 77,
\end{aligned}$$

$$\begin{aligned}
N_{11} = {} & 319489 \cdot 974849 \cdot 16798855634176047513 7\\
& \cdot 356084190644583392051 3 \cdot P_{564},
\end{aligned}$$

where P_{564} is prime with 564 decimal digits

$$\begin{aligned}
P_{564} = {} & 17346244717914755543025897086430977837742184472366408 46\\
& 49347019061363579192879108857591038330408837177983810 86\\
& 84515464219407129783061341898642808260145427587085892 43\\
& 87368556397311894886939915854550661114742021613255701 72\\
& 60564139394366945793220968665108959685482705388072645 82\\
& 85541519364019124649311825460928798157330577955733585 04\\
& 98227928009094287256759151891211862275171431922978810 09\\
& 79251036035496917279912663527358783236647193154777091 42\\
& 77453770382945849189175903251109393813224860442985739 71\\
& 65071105924446217754254070691304703466464360349138244 17\\
& 2330659883417 7.
\end{aligned}$$

References

[1] O. Ahmadi, I. E. Shparlinski, J. F. Voloch, *Multiplicative order of Gauss periods*, Intern. J. Number Theory, N.**4**, 2010, pp.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 Appl., N.**3**, 2005, pp.58-366.

[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, N.**3**, 1986, pp.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., N.**6**, 1999, pp.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., N.**2**, 2011, pp.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., N.**4**, 2012, pp.700-710.

[13] R. Popovych, *Elements of high order in finite fields of the form* $F_q[x]/(x^m - a)$, Finite Fields Appl., N.**1**, 2013, pp.86-92.

[14] D. Wiedemann, *An iterated quadratic extension of GF(2)*, Fibonacci Quart., N.**4**, 1988, pp.290-295.

Contact information

R. Popovych Lviv Polytechnic National University, Institute of Computer Technologies, Bandery Str., 12, Lviv, 79013, Ukraine
E-Mail(s): rombp07@gmail.com

Received by the editors: 26.02.2016
and in final form 12.03.2018.