ISSN 2075-9827 **e-ISSN 2313-0210**
Carpathian Math. Publ. 2015, **7** (2), 220–225
doi:10.15330/cmp.7.2.220-225

http://www.journals.pu.if.ua/index.php/cmp
Карпатські матем. публ. 2015, Т.7, №2, С.220–225

POPOVYCH R.

ON THE MULTIPLICATIVE ORDER OF ELEMENTS IN WIEDEMANN'S TOWERS OF FINITE FIELDS

We consider recursive binary finite field extensions $E_{i+1} = E_i(x_{i+1})$, $i \geq -1$, defined by D. Wiedemann. The main object of the paper is to give some proper divisors of the Fermat numbers N_i that are not equal to the multiplicative order $O(x_i)$.

Key words and phrases: finite field, multiplicative order, Wiedemann's tower.

Lviv Polytechnic National University, 12 Bandera str., 79013, Lviv, Ukraine
E-mail: rombp07@gmail.com

INTRODUCTION

High order elements are often needed in several applications that use finite fields [8, 9]. 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 reach 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 for special finite fields. We use F_q to denote finite field with q elements. Gao [5] gave an algorithm constructing high order elements for many (conjecturally all) general extensions F_{q^n} of finite field F_q with lower bound on the order $\exp(\Omega((\log m)^2/\log\log m))$. Voloch [13] proposed a method which constructs an element of order at least $\exp((\log m)^2)$ in finite fields from elliptic curves.

For special finite fields, it is possible to construct elements which can be proved to have much higher orders. Extensions connected with a notion of Gauss period are considered in [1, 11]. The lower bound on the order equals to $\exp(\Omega(\sqrt{m}))$. Extensions based on Kummer polynomials are of the form $F_q[x]/(x^m - a)$ [2, 3]. It is shown in [3] how to construct high order elements in such extensions with the condition $q \equiv 1(mod\ m)$. The lower bound $\exp(\Omega(m))$ is obtained in this case. The condition $q \equiv 1(mod\ m)$ for extensions based on Kummer polynomials is removed in [12].

Another less ambitious, but supposedly more important question, is to find primitive elements for a class of special finite fields. A polynomial algorithm that finds a primitive element in finite field of small characteristic is described in [6]. 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 some restrictions and as a consequence

УДК 512.624
2010 *Mathematics Subject Classification:* 11T30.
Scientific results, presented in this article, were obtained in the frame of research project number 0115U000446, 01.01.2015 - 31.12.2017, financially supported by the Ministry of Education and Science of Ukraine.

a lower bound on multiplicative order of some elements in binary recursive extensions of finite fields defined by Wiedemann [14]. The paper concerns with the open question posed by Wiedemann [10, problem 28]. Voloch [13] gave the first nontrivial estimate for the order of elements in this construction, namely $\exp(2^{2^i\delta})$, where δ is an absolute constant. However, the constant is unknown. Our bound does not depend on any unknown constant.

More precisely, we consider the following finite fields defined by Wiedemann that are constructed recursively:

$$x_{-1} = 1,\ E_{-1} = F_2(x_{-1}) = F_2,$$

for $i \geq -1$, $E_{i+1} = E_i(x_{i+1})$, where x_{i+1} satisfies the equation

$$x_{i+1}^2 + x_{i+1}x_i + 1 = 0. \tag{1}$$

So, we obtain the following tower of characteristic two finite fields:

$$F_2 \subset E_0 = F_2(x_0) \subset E_1 = E_0(x_1) \subset \dots$$

For comparison, the following finite fields are defined by Conway [14]:

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

for $i \geq -1$, $L_{i+1} = L_i(c_{i+1})$, where c_{i+1} satisfies the equation

$$c_{i+1}^2 + c_{i+1} + \prod_{j=-1}^{i} c_j = 0.$$

In this case, the following tower of finite fields of characteristic two arises:

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

From a point of view of applications such construction is very attractive, since we can perform operations with finite field elements recursively, and therefore effectively [7].

Note that the number of elements of the multiplicative group E_i^* ($i \geq 0$), that is the set of non-zero elements of the field E_i, 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 E_i^* ($i \geq 0$) is equal to $2^{2^{i+1}} - 1 = \prod_{j=0}^{i} N_j$. For example, $|E_0^*| = 2^{2^1} - 1 = 3$, $|E_1^*| = 2^{2^2} - 1 = 15 = 3 \cdot 5$, $|E_2^*| = 2^{2^3} - 1 = 255 = 3 \cdot 5 \cdot 17$.

1 PRELIMINARIES

We give below in Lemmas 1–9 auxiliary results for this paper.

Lemma 1 ([5]). *For $j \geq 1$ the following equality holds $N_j = \prod_{k=0}^{j-1} N_k + 2$.*

As a consequence of Lemma 1, we have the following lemma.

Lemma 2. *Numbers N_j ($j \geq 0$) are pair-wise coprime.*

Lemma 3 ([14]). *For $i \geq 0$, the following equality holds: $(x_i)^{N_i} = 1$.*

The multiplicative order of a field element x_i is defined to be the smallest nonnegative integer N_i such that $(x_i)^{N_i} = 1$. According to Lagrange theorem for finite groups, the above result implies that the order of x_i divides N_i. In the case where N_i is prime, x_i has order that precisely equals to N_i. The open question posed by Wiedemann [10, problem 28] is as follows: does the multiplicative order $O(x_i)$ of the element x_i equal to N_i. In any case, the order of x_i divides N_i.

Lemma 4. *Let $u_r = \prod_{i=0}^{r} x_i$ for $r = 0, 1 \dots$. The multiplicative order of element u_r equals to $O(u_r) = \prod_{i=0}^{r} O(x_i)$.*

Proof. Since the Fermat numbers are pair-wise coprime (see Lemma 2), the order of $u_r = \prod_{i=0}^{r} x_i$ is the product of the orders of x_i, $0 \le i \le r$. The number of elements of the multiplicative group E_i^* $(i = 0, 1, \dots)$ is equal to $\prod_{j=0}^{i} N_j$. As a corollary of Lemma 3 we have that the group E_i^* $(i = 0, 1, \dots)$ is an internal direct product of subgroups with $N_j (j = 0, \dots, i)$ elements. The element x_i belongs to the subgroup with the order N_i. □

We say that an element of a finite field is primitive if its order is the same as the number of nonzero field elements. If the order of x_i is, in fact, N_i for $0 \le i \le r$, then $u_r = \prod_{i=0}^{r} x_i$ is a primitive element in E_r, because $2^{2^{i+1}} - 1 = \prod_{j=0}^{i} N_j$. So, the given before Wiedemann's question can be reformulated as follows: is the element $u_r = \prod_{i=0}^{r} x_i$ primitive.

Lemma 5. *For $j \ge 2$, 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 [4, Theorem 1.3.5]) states: for $j \ge 2$, 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. □

Lemma 6. *Let K be a finite field of characteristic two and $x, y \in K$. If*

$$y^2 = yx + 1, \tag{2}$$

then

$$y^{2^k} = yx^{2^k - 1} + \sum_{j=1}^{k} x^{2^k - 2^j} \tag{3}$$

for any positive integer k.

Proof. By induction on k. For $k = 1$ we obtain the equality (2).

Suppose the equality (2) holds for some positive integer k. Then

$$y^{2^{k+1}} = \left(y^{2^k}\right)^2 = \left(yx^{2^k - 1} + \sum_{j=1}^{k} x^{2^k - 2^j}\right)^2 = y^2 x^{2^{k+1} - 2} + \sum_{j=1}^{k} x^{2^{k+1} - 2^{j+1}}.$$

Taking into account (2), we have

$$y^{2^{k+1}} = yx^{2^{k+1} - 1} + \sum_{j=1}^{k+1} x^{2^{k+1} - 2^j},$$

that is the equality (3) is true for $k + 1$ as well. □

Lemma 7. *The multiplicative order $O(x_i) = N_i$ for $0 \le i \le 11$.*

Proof. For $0 \le i \le 4$ Fermat numbers are prime [4]: $N_0 = 3$, $N_1 = 5$, $N_2 = 17$, $N_3 = 257$, $N_4 = 65537$. Therefore clearly for these numbers, as a consequence of Lemma 3, the order of the element x_i coincides with the correspondent Fermat number, that is $O(x_i) = N_i$.

The rest of the proof uses computer calculations. We perform calculations of order of the element x_i for $5 \le i \le 11$. In this case Fermat numbers are completely factored into primes [5].

Using the mentioned factorizations, we calculate x_i in the power N_i/q for any prime divisor q of the number N_i. Really, if an element in the power N_i/q is not equal to one, then the element in the power of any divisor of N_i/q is also not equal to one. As a result we obtain that for $5 \leq i \leq 11$ the order of element x_i is not less than N_i, namely precisely equals to N_i. □

Lemma 8. *For $i \geq 0$ the inverse element to the element x_i equals to $(x_i)^{-1} = x_i + x_{i-1}$.*

Proof. Based on the given in the introduction recursive equation (1), that defines the Wiedemann's tower, we have $x_i(x_i + x_{i-1}) = (x_i)^2 + x_i x_{i-1} = 1$. Hence, the element x_i is the inverse to the element $x_i + x_{i-1}$. □

Lemma 9. *The following equalities hold for $i \geq 1$:*

$$x_i^2 = x_i x_{i-1} + 1, \tag{4}$$

$$x_i^3 = x_{i-1}(x_{i-2}x_i + 1), \tag{5}$$

$$x_i^5 = x_{i-1}[(x_{i-2}^2 + 1)x_{i-1}x_i + x_{i-2}x_{i-1} + 1]. \tag{6}$$

Proof. The equality (4) follows directly from (1). Using (4) for x_i^2 consequently two times, we obtain

$$x_i^3 = x_i^2 \cdot x_i = x_{i-1}x_i^2 + x_i = x_{i-1}^2 x_i + x_{i-1} + x_i.$$

Substituting now the value of x_{i-1}^2 from (4), leads to (5). Using (4) and (5), we have

$$\begin{aligned} x_i^5 = x_i^3 \cdot x_i^2 = x_{i-1}(x_{i-2}x_i + 1)(x_{i-1}x_i + 1) &= x_{i-1}(x_{i-2}x_{i-1}x_i^2 + x_{i-2}x_i + x_{i-1}x_i + 1) \\ &= x_{i-1}(x_{i-1}^2 x_{i-2}x_i + x_{i-2}x_{i-1} + x_{i-2}x_i + x_{i-1}x_i + 1). \end{aligned}$$

Substituting now the value of x_{i-1}^2 from (4), gives (6). □

2 MAIN RESULTS

We give in this section in Theorems 1–3 and Corollary main results of this paper.

Theorem 1. *The order $O(x_i)$ ($i \geq 0$) cannot be a divisor of a number of the form $2^k + 1$, where k is a positive integer and $k < 2^i$.*

Proof. By induction on i. For $0 \leq i \leq 11$ it is true according to Lemma 7. Let the assertion holds for numbers from 12 to $i - 1$.

Show by the way of contradiction that the assertion holds for i as welll. Assume that $O(x_i)$ divides $2^k + 1$, where $k < 2^i$. Then $(x_i)^{2^k+1} = 1$ and Lemma 8 gives

$$(x_i)^{2^k} = (x_i)^{-1} = x_i + x_{i-1}. \tag{7}$$

On the other hand, putting in (3) $y = x_i$, $x = x_{i-1}$, we have

$$(x_i)^{2^k} = x_i(x_{i-1})^{2^k-1} + \sum_{j=1}^{k}(x_{i-1})^{2^k-2^j}. \tag{8}$$

Comparing coefficients near x_i in (7) and (8), we obtain $(x_{i-1})^{2^k-1} = 1$. Hence, $O(x_{i-1})$ divides $2^k - 1$. At the same time, by Lemma 3, $O(x_{i-1})$ is a divisor of $2^{2^{i-1}} + 1$. Then $O(x_{i-1})$ divides the sum of numbers $2^{2^{i-1}} + 1$ and $2^k - 1$, that is equal to $S = 2^{2^{i-1}} + 2^k$. Consider the following three possible cases.

1) If $k = 2^{i-1}$, then $S = 2^{2^{i-1}} + 2^k = 2^{2^{i-1}+1}$. In this case $O(x_{i-1})$ equals to a power of two. This contradicts to the fact that $O(x_{i-1})$ must divide $2^{2^{i-1}} + 1$.

2) If $k < 2^{i-1}$, then $S = 2^k(2^{2^{i-1}-k} + 1)$. As 2^k is coprime with $2^{2^{i-1}} + 1$, the order $O(x_{i-1})$ divides $2^{2^{i-1}-k} + 1$. Since $k \geq 1$, the inequality $2^{i-1} - k < 2^{i-1}$ holds, a contradiction with the induction hypothesis.

3) If $k > 2^{i-1}$, then $S = 2^{2^{i-1}}(2^{k-2^{i-1}} + 1)$. As $2^{2^{i-1}}$ is coprime with $2^{k-2^{i-1}} + 1$, the order $O(x_{i-1})$ is a divisor of $2^{k-2^{i-1}} + 1$. Since $k < 2^i$, the inequality $k - 2^{i-1} < 2^{i-1}$ is true, a contradiction with the induction hypothesis.

Therefore, we obtain a contradiction in all three possible cases, what shows that the assertion also holds for i. □

Theorem 2. *The order $O(x_i)$ ($i \geq 0$) cannot be a divisor of a number of the form $s \cdot 2^k + 1$, where $s = 3, 5$ and k is a non negative integer.*

Proof. By the way of contradiction. If $O(x_i)$ is a divisor of a number of the form $s \cdot 2^k + 1$, then $(x_i)^{s \cdot 2^k + 1} = 1$ and clearly

$$(x_i)^{s \cdot 2^k} = (x_i)^{-1}. \tag{9}$$

Denote $t = 2^i - k$. Then $2^{2^i} = 2^t \cdot 2^k$. Powering left and right side of the equation (9) to 2^t and taking into account $(x_i)^{2^{2^i}} = (x_i)^{-1}$, we obtain

$$(x_i)^{2^t} = (x_i)^s.$$

Consider the case $s = 3$. According to Lemma 6

$$(x_i)^{2^t} = x_i(x_{i-1})^{2^t - 1} + \sum_{j=1}^{t} (x_{i-1})^{2^t - 2^j}. \tag{10}$$

Comparing coefficients near x_i on the right side of (10) and (5), we have

$$(x_{i-1})^{2^t - 2} = x_{i-2}.$$

Since $x_{i-2} \neq 1$ and, by lemma 2, Fermat numbers are coprime, we have the trivial intersection of cyclic subgroups $\langle x_{i-1} \rangle \bigcap \langle x_{i-2} \rangle = 1$, a contradiction. As a consequence, $O(x_i)$ ($i \geq 0$) cannot be a divisor of a number of the form $3 \cdot 2^k + 1$, where k is a non negative integer.

Consider now the case $s = 5$. Comparing coefficients near x_i on the right side of (10) and (6), we obtain

$$(x_{i-1})^{2^t - 3} = (x_{i-2})^2 + 1.$$

Since $(x_{i-2})^2 + 1 = x_{i-2}x_{i-3} \neq 0$, we have $(x_{i-2})^2 + 1 \in [F_2(x_{i-2})]^*$. Note that $(x_{i-2})^2 + 1 \neq 1$, because $(x_{i-2})^2 \neq 0$. The fact: N_{i-1} is coprime with $N_{i-2}N_{i-3}$ (see lemma 2), leads to $\langle x_{i-1} \rangle \bigcap [F_2(x_{i-2})]^* \neq 1$, a contradiction. Therefore, $O(x_i)$ ($i \geq 0$) cannot be a divisor of a number of the form $5 \cdot 2^k + 1$, where k is a non negative integer. □

Theorem 3. *The order of element x_i equals to N_i for $0 \leq i \leq 11$ and is at least $7 \cdot 2^{i+2} + 1$ for $i \geq 12$.*

Proof. By Lemma 7 $O(x_i) = N_i$ holds for $0 \leq i \leq 11$. Show now that $O(x_i) \geq 7 \cdot 2^{i+2} + 1$ for $i \geq 12$. If $(x_i)^{n_i} = 1$, then, by the Lagrange theorem for finite groups, n_i divides N_i. According to Lemma 3, $n_i = s \cdot 2^{i+2} + 1$, where s is a positive integer. By Theorem 1, s can not equal to 1, 2 or 4, and by Theorem 2 s can not equal to 3, 5 or 6, that is $s \geq 7$. Hence, the result follows. □

Corollary. *The order of element* $u_r = \prod_{i=0}^{r} x_i$ *equals to* $\prod_{i=0}^{r} N_i$ *for* $0 \le r \le 11$ *and is at least* $\prod_{i=0}^{11} N_i \cdot \prod_{i=12}^{r} (7 \cdot 2^{i+2} + 1)$ *for* $r \ge 12$.

Proof. According to Lemma 4, we have the equality $O(u_r) = \prod_{i=0}^{r} O(x_i)$. Applying now Theorem 3, we obtain given in the formulation of the corollary bounds on the order. □

REFERENCES

[1] Ahmadi O., Shparlinski I. E., Voloch J. F. *Multiplicative order of Gauss periods*. Intern. J. Number Theory 2010, **6** (4), 877–882. doi: 10.1142/S1793042110003290

[2] Burkhart J. F. et al. *Finite field elements of high order arising from modular curves*. Des. Codes Cryptogr. 2009, **51** (3), 301–314. doi:10.1007/s10623-008-9262-y

[3] Cheng Q. *On the construction of finite field elements of large order*. Finite Fields Appl. 2005, **11** (3), 358–366. doi:10.1016/j.ffa.2005.06.001

[4] Crandall R., Pomerance C. Prime Numbers, A Computational Perspective. Springer-Verlag, New York, 2005.

[5] Gao S. *Elements of provable high orders in finite fields*. Proc. Amer. Math. Soc. 1999, **127** (6), 1615–1623. doi:10.1090/S0002-9939-99-04795-4

[6] Huang M.-D., Narayanan A. K. *Finding primitive elements in finite fields of small characteristic*. arXiv 1304.1206 2013.

[7] Ito H., Kajiwara T., Song H. A. *A tower of Artin-Schreier extensions of finite fields and its applications*. JP J. Algebra Number Theory Appl. 2011, **22** (2), 111–125.

[8] Lidl R., Niederreiter H.. Finite Fields. Cambridge Univ. Press, Cambridge, 1997.

[9] Mullen G.L., Panario D. Handbook of finite fields. CRC Press, Boca Raton, FL, 2013.

[10] Mullen G. L., Shparlinski I. E. Open problems and conjectures in finite fields. In: Cohen S.D., Niederreiter H. (Eds.) Finite Fields and Applications, London Math. Soc. Lecture Note Ser., **233**. Cambridge Univ. Press, Cambridge, 1996.

[11] Popovych R. *Elements of high order in finite fields of the form* $F_q[x]/\Phi_r(x)$. Finite Fields Appl. 2012, **18** (4), 700–710. doi:10.1016/j.ffa.2012.01.003

[12] Popovych R. *Elements of high order in finite fields of the form* $F_q[x]/(x^m - a)$. Finite Fields Appl. 2013, **19** (1), 86–92. doi:10.1016/j.ffa.2012.10.006

[13] Voloch J.F. *Elements of high order on finite fields from elliptic curves*. Bull. Austral. Math. Soc. 2010, **81** (3), 425–429. doi:10.1017/S0004972709001075

[14] Wiedemann D. *An iterated quadratic extension of GF(2)*. Fibonacci Quart. 1988, **26** (4), 290–295.

Received 01.07.2015

Попович Р. *Про мультиплікативний порядок елементів у вежах Відемана скінченних полів* // Карпатські матем. публ. — 2015. — Т.7, №2. — С. 220–225.

Розглядаються рекурсивні двійкові розширення скінченних полів $E_{i+1} = E_i(x_{i+1})$, $i \ge -1$, визначені Д. Відеманом. Основна мета роботи — описати деякі власні дільники чисел Ферма N_i, які не дорівнюють мультиплікативному порядку $O(x_i)$.

Ключові слова і фрази: скінченне поле, мультиплікативний порядок, вежа Відемана.