ISSN 2075-9827 **e-ISSN 2313-0210**
Carpathian Math. Publ. 2022, **14** (1), 238–246
doi:10.15330/cmp.14.1.238-246

https://journals.pnu.edu.ua/index.php/cmp
Карпатські матем. публ. 2022, Т.14, №1, С.238–246

Elements of high order in finite fields specified by binomials

Bovdi V.[1], Diene A.[1], Popovych R.[2]

Let F_q be a field with q elements, where q is a power of a prime number $p \geq 5$. For any integer $m \geq 2$ and $a \in F_q^*$ such that the polynomial $x^m - a$ is irreducible in $F_q[x]$, we combine two different methods to explicitly construct elements of high order in the field $F_q[x]/\langle x^m - a\rangle$. Namely, we find elements with multiplicative order of at least $5^{\sqrt[3]{m/2}}$, which is better than previously obtained bound for such family of extension fields.

Key words and phrases: finite field, multiplicative order, element of high multiplicative order, binomial.

[1] United Arab Emirates University, Al Ain, United Arab Emirates
[2] Lviv Polytechnic National University, Lviv, Ukraine
E-mail: vbovdi@gmail.com (Bovdi V.), adiene@uaeu.ac.ae (Diene A.), rombp07@gmail.com (Popovych R.)

1 Introduction

The problem of efficiently constructing a primitive element for a given finite field is notoriously difficult computational task of finite fields. That is why one considers a less restrictive question, namely to find an element with "high" or "large" multiplicative order. Based on [5, p. 1615], by "large order" (high order, exponential order) of an element in the finite field F_{q^m} of q^m elements we mean that the order of this element must be bigger than every polynomial in $\log(q^m)$ as $q^m \to \infty$. In general, we are not required to compute the exact order of such an element, but it is sufficient to obtain its lower bound.

High order elements in finite fields are very useful in several applications, such as cryptography, coding theory, pseudo random number generation and combinatorics.

S. Gao [5] provided an algorithm for constructing high order elements for many (conjecturally all) general extensions F_{q^m} of a finite field F_q with the following lower bound $\exp(\Omega((\log m)^2/\log\log m))$ on the order. This bound was improved in [15]. J.F. Voloch [18] proposed a method which constructs an element of order of at least $\exp(\Omega((\log m)^2))$. However, for some classes of finite fields it is possible to construct elements of much higher orders (for example, see [1, 6, 13, 14, 17]). In these articles, extensions connected with cyclotomic polynomials are considered and elements of order bounded by $\exp(\Omega(\sqrt{m}))$ are constructed. Note that this bound is much better than the ones we mentioned previously.

Some another classes of extensions based on the Kummer or Artin-Schreier polynomials were considered in [4, 9, 12]. The best known lower bound of the order (see [12, Theorem 1]) for extensions, specified by Kummer polynomials, is $2^{\lfloor\sqrt[3]{2m}\rfloor}$, where $\lfloor\sqrt[3]{2m}\rfloor$ is the highest integer less or equal to $\sqrt[3]{2m}$. In our current article, we continue this line of investigation.

УДК 511.2, 512.624
2020 *Mathematics Subject Classification:* 11T30, 11Y99, 11T06, 20K01, 13M10.

2 Main Results

Let $p, q, m, n \in \mathbb{N}$, where p is an odd prime, $q = p^n$ and $m \geq 2$. Let F_q be a finite field of q elements and let $a \in F_q^*$ such that $x^m - a$ is an irreducible polynomial over F_q.

Let $F_{q^m} = F_q(\theta) = F_q[x]/\langle x^m - a\rangle$ be a field extension of F_q based on the irreducible binomial (Kummer polynomial) $x^m - a$, where $\langle f(x)\rangle$ is an ideal of $F_q[x]$ generated by $f(x) \in F_q[x]$ and θ is the coset of x in $F_q[x]/\langle x^m - a\rangle$.

We widely use (see Lemma 1) the following fact from [11]. Let F_q be a finite field of characteristic $p \geq 5$. There exist infinitely many natural numbers m and $a = a(m) \in F_q^*$, such that $x^m - a \in F_q[x]$ is an irreducible polynomial. Such elements $a = a(m) \in F_q^*$ are called *m-related*.

Our main results use the fact that the extension degree $m = k \cdot l$ is a product of two numbers, where $k > 1$ is a divisor of $q - 1$, and $l \geq 1$ is the order of the number q modulo m. Using a special representation of elements of the group $\langle q \pmod m\rangle$ (see [12, Lemma 4, p. 88]), we deduce the following: if $q - 1$ has a "large" divisor k, we use for the construction of the method similar to the case $F_q[x]/\langle x^m - a\rangle$ with the condition $q \equiv 1 \pmod m$ or to the case $F_p[x]/\langle x^p - x - a\rangle$ (see [4, p. 363–365]); if $q - 1$ does not have a big divisor k, then $l = m/k$ is large, and we use for the construction of the method similar to the case $F_q[x]/\langle x^{r-1} + \cdots + x + 1\rangle$ (see [1, 13]). We take in both cases a linear binomial in some power of θ and all consecutive qth powers of it (the so called conjugates), that also belong to the group generated by the binomial, and construct their distinct products.

In the first case, when $q \equiv 1 \pmod k$, the conjugates of $\theta^l + b$, $b \in F_q^*$, are linear binomials in θ^l. The idea was introduced by P. Berrizbeitia [3] as an improvement of the AKS primality proving algorithm and developed by several authors (see [4, 13] and also the survey article [7]). Our first result, which uses the first mentioned method, is the following.

Theorem 1. *Let $q = p^n$, where $p \geq 5$ is a prime and let $m = k \cdot l \in \mathbb{N}$ such that $k > 1$ is a divisor of $q - 1$, and $l \geq 1$ is the multiplicative order of $q \pmod m$. Let $a \in F_q^*$ be an m-related element (i.e. $x^m - a \in F_q[x]$ is an irreducible polynomial) and let the element θ define the field extension $F_q(\theta) = F_q[x]/\langle x^m - a\rangle$.*

If $b \in F_q^*$, then the multiplicative order of $\theta^l + b \in F_q(\theta)$ is at least

$$\mathfrak{d}_1 := \max_{0 \leq d_- \leq d < k} \left\{ \binom{k}{d} \binom{d}{d_-} \binom{2k - d - d_- - 1}{k - d - 1} \right\}.$$

Moreover, if $k \geq 70$, then $\mathfrak{d}_1 \geq 5^k$.

Note that $\mathfrak{d}_1 \geq \frac{5{,}7556^k}{30k^{3/2}}$ for $k \geq 8$ by [16, Theorem 1, p. 23, Corollary 2, p. 25]. It is easy to see that our lower bound is better for $k \geq 70$.

Hence, we derive a lower bound on the order of $\theta^l + b$, which depends on k.

In the second case, the conjugates of $\theta + b$ are non-linear polynomials in θ. The idea was introduced by J. von zur Gathen and I. Shparlinski for the fields based on cyclotomic polynomials [6], and developed in [1, 13, 14].

Let

$$\mathbf{T} = \Big\{ (u_0, \ldots, u_{l-1}) \in \mathbb{Z}^l : \sum_{i=0}^{l-1} (i \cdot k + 1) u_i < m, \quad 0 \leq u_0, \ldots, u_{l-1} \leq p - 1 \Big\}. \tag{1}$$

Our second result, which uses the second mentioned above method, is the following.

Theorem 2. *Let $q = p^n$, where $p \geq 5$ is a prime and let $m = k \cdot l \in \mathbb{N}$ such that $k > 1$ is a divisor of $q-1$, and $l \geq 1$ is the multiplicative order of $q \pmod m$. Let $a \in F_q^*$ be an m-related element (i.e. $x^m - a \in F_q[x]$ is an irreducible polynomial) and let the element θ define the field extension $F_q(\theta) = F_q[x]/\langle x^m - a\rangle$.*

If $b \in F_q^*$, then the multiplicative order of $\theta + b \in F_q(\theta)$ is at least $\mathfrak{d}_2 := |T| \geq 5^{\sqrt{l/2}}$.

Moreover:

(i) if $l \geq p^2 + 1$, then

$$\mathfrak{d}_2 \geq \left(\frac{p(p-1)}{160(l-1)}\right)^{\sqrt{p}} \exp\left(2.5 \cdot \sqrt{(1-\frac{1}{p})(l-1)}\right);$$

(ii) if $l < p + 1$, then

$$\mathfrak{d}_2 \geq \frac{\exp\left(2.5 \cdot \sqrt{l-1}\right)}{13(l-1)}.$$

Items *(i)* and *(ii)* of Theorem 2 are slightly better comparatively with $5^{\sqrt{l/2}}$ lower bounds on $\mathfrak{d}_2$, but not so explicit and not for all values of l. To prove these items we use Lemmas 4, 5 and 6. We take $\pi\sqrt{2/3} \approx 2.5$ to simplify formulas in *(i)* and *(ii)*.

Hence, we obtain lower bounds on the order of the element $\theta + b$, which depend on l or on l and p.

Our third result, which takes together our first and second results, is the following.

Theorem 3. *Let $q = p^n$, where $p \geq 5$ is a prime and let $m = k \cdot l \in \mathbb{N}$ such that $k > 1$ is a divisor of $q-1$, and $l \geq 1$ is the multiplicative order of $q \pmod m$. Let $a \in F_q^*$ be an m-related element (i.e. $x^m - a \in F_q[x]$ is an irreducible polynomial) and let the element θ define the field extension $F_q(\theta) = F_q[x]/\langle x^m - a\rangle$.*

It is always possible to construct explicitly in the field $F_q(\theta)$ an element of which the multiplicative order is at least $\max\{\mathfrak{d}_1, \mathfrak{d}_2\}$.

Moreover, if $k \geq 70$, then the multiplicative order is at least $5^{\sqrt[3]{m/2}}$.

The best previously known lower bound on the order of elements for finite field extensions defined by a binomial is equal to $2^{\sqrt[3]{2m}} = 2,3948^{\sqrt[3]{m}}$ (see [12, Theorem 1, p. 87]). Our Theorem 3 gives a new bound $5^{\sqrt[3]{m/2}} = 3,5873^{\sqrt[3]{m}}$, which is an improvement of $2^{\sqrt[3]{2m}}$.

3 Lemmas and proofs

The multiplicative group $F_{q^m}^*$ of the finite field F_{q^m} is cyclic of order $q^m - 1$ with $\varphi(q^m - 1)$ generators which are called primitive elements, where φ is the Euler totient function. For an element g of a group G, we denote by $\langle g\rangle$ the cyclic subgroup generated by g.

Let c be a fixed positive integer. A partition $\mathcal{P}(c)$ of c is a sequence of non-negative integers $u_1, \ldots, u_c$ such that

$$c = \sum_{j=1}^{c} j u_j. \tag{2}$$

We define the following three numbers

$$\mathfrak{u}(c), \quad \mathfrak{u}(c,d), \quad \mathfrak{q}(c,d) \tag{3}$$

related to some subsets of the set of all partitions given by (2):

(P_1) $\mathfrak{u}(c)$ is the number of all partitions $\mathcal{P}(c)$;

(P_2) $\mathfrak{u}(c,d)$ is the number of those partitions $\mathcal{P}(c)$ for which $u_1,\ldots,u_c \leq d$ (i.e. each part appears no more than d times);

(P_3) $\mathfrak{q}(c,d)$ is the number of those partitions $\mathcal{P}(c)$ for which $u_j = 0$ if $j \equiv 0 \pmod{d}$, (i.e. each part of which is not divisible by d).

In a finite field of characteristic two, the polynomial $x^m - a$ is irreducible if and only if $m = 1$. For a finite field of an odd characteristic the question when the polynomial $x^m - a$ is irreducible was done by Panario and Thomson [11]. In the case $p = 3$ the only possible extension is for $m = 2$, namely the irreducible polynomial $x^2 - 2$. If $p \geq 5$, then we can construct the extensions for infinitely many m.

Lemma 1 ([11, Theorem 2, p. 3]). *Let F_q be a finite field of characteristic $p \geq 5$.*

For $m \not\equiv 0 \pmod 4$ there exists an irreducible binomial over F_q of degree m if and only if every prime factor of m is also a prime factor of $q-1$.

For $m \equiv 0 \pmod 4$ there exists an irreducible binomial over F_q of degree m if and only if $q \equiv 1 \pmod 4$ and every prime factor of m is also a prime factor of $q-1$.

Note that [11] not only provides the possible degrees m such that irreducible binomials $x^m - a$ exist, but also provides a procedure to construct the m-related elements $a = a(m)$.

Lemma 2 ([12, Lemma 4, p. 88]). *Let $m \geq 2$ and let $a \in F_q^*$ be an m-related element (i.e. $x^m - a \in F_q[x]$ is an irreducible polynomial). If $m = k \cdot l \in \mathbb{N}$, in which k is a divisor of $q-1$ and l is the order of q modulo m, then $\langle q \rangle \leq \mathbb{Z}_m^*$ can be written as*

$$\langle q \rangle = \{\overline{i \cdot k + 1} : i = 0,\ldots,l-1\}.$$

The next result below is a typical tool how to construct high order elements (see [4,5,10]).

Lemma 3. *Let $m \geq 2$ and let $f(x) \in F_q[x]$ be an irreducible polynomial of degree m. Let $g(x), h(x) \in F_q[x]$ such that $g(x) \neq h(x)$. If $\deg(g(x))$ and $\deg(h(x))$ are less than m, then*

$$g(x) + \langle f(x) \rangle \neq g(x) + \langle f(x) \rangle \in F_q[x]/\langle f(x) \rangle.$$

Lemma 4 (Glaisher, 1883, see [2, Corollary 1.3, p. 6.]). *The number of partitions $\mathcal{P}(n_0)$ of $n_0 \in \mathbb{N}$ not containing d_0 equal parts is equal to the number of partitions $\mathcal{P}(n_0)$ of n_0 with no part divisible by d_0, i.e.*

$$\mathfrak{u}(n_0, d_0 - 1) = \mathfrak{q}(n_0, d_0).$$

Lemma 5 ([8, Theorem 5.1]). *For all integers $d_0 > 1$ and $n_0 \geq d_0^2$, we have*

$$\left(\frac{d_0(d_0-1)}{160 n_0}\right)^{\sqrt{d_0}} \exp\left(2.5 \cdot \sqrt{(1 - \frac{1}{d_0}) n_0}\right) < \mathfrak{q}(n_0, d_0).$$

Lemma 6 ([8, Theorem 4.2]). *For all integers $n_0 > 1$*

$$\frac{\exp\left(2.5 \cdot \sqrt{n_0}\right)}{13 n_0} < \mathfrak{u}(n_0).$$

Proof of Theorem 1. Since k is a divisor of $q-1$, then, according to Lemma 1, the binomial $y^k - a$ is irreducible over $F_q[y]$. Set $\eta = \theta^l$. Clearly, $\eta^k = \theta^m = a$, and $F_q(\eta) = F_q[y]/\langle y^k - a\rangle$ is a subfield of $F_q(\theta)$.

Consider $\eta + b$ (a linear binomial in the power of $\eta = \theta^l$) and consequential qth powers (conjugates) of it that belong to the group generated by this binomial. Write $q - 1 = kh$ for some integer h. Then $\eta^q + b = (\eta^k)^h\eta + b = a^h\eta + b$ and the conjugates of $\eta + b$ are equal to

$$(\eta + b)^{q^i} = a^{hi}\eta + b, \quad i = 0, \dots, k-1.$$

Consider the subgroup $H = \langle a^{hi}\eta + b : i = 0, \dots, k-1\rangle \leq \langle \eta + b\rangle \leq F_q^*(\eta)$. For a vector $\alpha = (u_0, \dots, u_{k-1}) \in \mathbb{Z}^k$, we define the product

$$\mathrm{P}(\alpha) = \prod_{i=0}^{k-1}(a^{hi}\eta + b)^{u_i} \in H. \tag{4}$$

The next combinatorial problem was introduced by J.F. Voloch in order to improve the AKS primality proving algorithm and this method has been developed by several authors (see surveys [7, p. 31–32] and [16]).

This problem consists of finding for a fix $k \in \mathbb{N}$ two non-negative integers $0 \leq d_- \leq d < k$ with maximal possible value of the product $\binom{k}{d_-}\binom{d}{d_-}\binom{k-d_--d-1}{k-d-1}$ of the following three binomial coefficients $\binom{k}{d_-}$, $\binom{d}{d_-}$ and $\binom{k-d_--d-1}{k-d-1}$.

It is easy to check that this product $\binom{k}{d_-}\binom{d}{d_-}\binom{k-d_--d-1}{k-d-1}$ is the cardinality of the set $S = \{(u_0, u_1, \dots, u_{k-1}) \in \mathbb{Z}^k\}$ with the following properties:

(i) the number of negative components equals d_-,

(ii) the sum of absolute values of negative components $\sum_{i,u_i<0} |u_i| \leq d$,

(iii) the sum of positive components $\sum_{i,u_i\geq 0} u_i \leq k - 1 - d$,

where $0 \leq d_- \leq d < k$.

Indeed, to specify the element of this set, we choose at first places, where vector values are negative: this takes into account the factor $\binom{k}{d_-}$. Then we choose values of negative elements so that the sum of their absolute values does not exceed d: this takes into account the factor $\binom{d}{d_-}$. Finally, we choose non-negative vector values at $k - d_-$ places, so that their sum does not exceed $k - 1 - d$: this takes into account the factor $\binom{k-d_-+k-1-d}{k-1-d}$.

For each $(u_0, u_1, \dots, u_{k-1}) \in S$ we consider the product (4) and claim that two different vectors $(u_0, u_1, \dots, u_{k-1})$ and $(v_0, v_1, \dots, v_{k-1})$ from S give different values of P.

Let $\alpha = (u_0, \dots, u_{k-1}), \beta = (v_0, \dots, v_{k-1}) \in S$ such that $\alpha \neq \beta$ and $P(\alpha) = P(\beta)$ (see (4)). Since $y^k - a \in F_q[y]$ is the characteristic polynomial of η, therefore

$$\prod_{i=0}^{k-1}(a^{hi}y + b)^{u_i} \equiv \prod_{i=0}^{k-1}(a^{hi}y + b)^{v_i} \pmod{\langle y^k - a\rangle}$$

and, as a consequence,

$$f_1(y) \equiv f_2(y) \pmod{\langle y^k - a\rangle}, \tag{5}$$

where

$$f_1(y) := \prod_{\substack{0\le i\le k-1,\\ 0\le u_i}} (a^{hi}y+b)^{u_i} \prod_{\substack{0\le i\le k-1,\\ 0> v_i}} (a^{hi}y+b)^{|v_i|},$$
$$f_2(y) := \prod_{\substack{0\le i\le k-1,\\ u_i<0}} (a^{hi}y+b)^{|u_i|} \prod_{\substack{0\le i\le k-1,\\ v_i\ge 0}} (a^{hi}y+b)^{v_i}.$$

Using (5) and the facts that

$$\deg(f_1(y)) = \sum_{\substack{0\le i\le k-1,\\ u_i\ge 0}} u_i + \sum_{\substack{0\le i\le k-1,\\ v_i<0}} |v_i| \le (k-1-d)+d = k-1,$$
$$\deg(f_2(y)) = \sum_{\substack{0\le i\le k-1,\\ u_i\le 0}} |u_i| + \sum_{\substack{0\le i\le k-1,\\ v_i\ge 0}} v_i \le d+(k-1-d) = k-1,$$

we conclude that $f_1(y) = f_2(y)$ from Lemma 3.

Moreover, each factor $a^{hi}y+b$ in $f_1(y)$ $(= f_2(y))$ is irreducible and $a^{hi}y \ne a^{hj}y$ for $i \ne j$. Since $F_q[y]$ is a unique factorization ring, we obtain a contradiction.

Hence, the number of $\alpha \in S$ such that $P(\alpha) \in H$ (see (4)) is equal to the cardinality of S. We choose d_- and d to obtain maximum of elements in S. As a result, $\eta + b$ has the multiplicative order at least $\mathfrak{d}_1$. □

Proof of Theorem 2. According to Lemma 2, for each $z \in \{0,\dots,l-1\}$ there exist unique $i \in \{0,\dots,l-1\}$ and $j = j(i) \in \mathbb{Z}$, such that $q^z = (i\cdot k+1) + j\cdot m$. Then conjugates of element $\theta + b$ are equal to

$$(\theta+b)^{q^z} = \theta^{q^z} + b = (\theta^m)^j\theta^{i\cdot k+1} + b = a^j\theta^{i\cdot k+1} + b \in \langle \theta+b\rangle.$$

Similarly, as in the proof of Theorem 1 (see also (1)), for a vector $\alpha = (u_0,\dots,u_{l-1}) \in \mathbf{T}$ we define the product

$$\mathrm{P}(\alpha) = \textstyle\prod_{i=0}^{l-1}(a^j\theta^{ik+1}+b)^{u_i} \in \langle \theta+b\rangle.$$

We claim that if $\beta = (v_0,\dots,v_{l-1}) \in \mathbf{T}$ is distinct from $\alpha \in \mathbf{T}$, then $P(\alpha) \ne P(\beta)$.

Indeed, let $P(\alpha) = P(\beta)$. Set

$$f_1(x) := \prod_{i=0}^{l-1}(a^jx^{i\cdot k+1}+b)^{u_i} \in F_q[x] \quad \text{and} \quad f_2(x) := \prod_{i=0}^{l-1}(a^jx^{i\cdot k+1}+b)^{v_i} \in F_q[x].$$

Clearly, $\deg(f_1(x)) = \sum_{i=0}^{l-1}(ik+1)u_i < m$ and $\deg(f_1(x)) = \sum_{i=0}^{l-1}(ik+1)u_i < m$. Since $x^m - a$ is the characteristic polynomial of θ, then

$$f_1(x) \equiv f_2(x) \pmod{\langle x^m - a\rangle},$$

so $f_1(x) = f_2(x)$ by Lemma 3.

Note that $F_q[x]$ is a unique factorization ring. Let r be the smallest integer for which $u_r \ne v_r$ and, say $u_r > v_r$, in which $u_i \in \alpha$ and $v_i \in \beta$. After removing common factors on both sides of the equation $f_1(x) = f_2(x)$, we observe that

$$(a^{j_r}x^{r\cdot k+1}+b)^{u_r-v_r} \prod_{i\ge r+1}^{l-1}(a^{j_i}x^{i\cdot k+1}+b)^{u_i} = \prod_{i\ge r+1}^{l-1}(a^{j_i}x^{ir+1}+b)^{v_i}. \tag{6}$$

The absolute term for the polynomial $\prod_{i\geq r+1}^{l-1}(a^{j_i}x^{i\cdot k+1}+b)^{u_i}$ we denote by c. Then there is the term $(u_r-v_r)a^{j_r}b^{u_r-v_r-1}cx^{r\cdot k+1}$ in the polynomial on the left side of (6) with the minimal non-zero power of x. Since $0\leq u_r,v_r\leq p-1, u_r\neq v_r, a,b,c\neq 0$, the term is non-zero. This term does not occur on the right side, which makes the identity (6) impossible. Hence, products, corresponding to distinct solutions, cannot be equal. Consequently, the multiplicative order of $\theta+b$ in $F_q(\theta)=F_q[x]/\langle x^m-a\rangle$ is at least $\mathfrak{d}_2:=|T|$.

Let $\tau\in[2,p-1]$ be an integer. Let us choose the largest integer $\alpha>0$ such that

$$\sum_{i=0}^{\alpha}(i\cdot k+1)(\tau-1)<m,\quad k\geq 2.$$

Obviously,

$$\sum_{i=0}^{\alpha}(i\cdot k+1)(\tau-1)=\frac{(\tau-1)(\alpha k+2)(\alpha+1)}{2}<\frac{(\tau-1)k(\alpha+1)^2}{2}.$$

If $\alpha:=\lfloor\sqrt{\frac{2l}{\tau-1}}-1\rfloor$, then $(\tau-1)k(\alpha+1)^2\leq 2m$ and for integers

$$u_i\in\begin{cases}[0,\tau-1] & \text{for}\quad i=0,\dots,\alpha,\\ 0 & \text{for}\quad i=\alpha+1,\dots,l-1,\end{cases}$$

the vector $(u_0,\dots,u_{l-1})$ belongs to the set T. The number of such vectors is $\tau^{\alpha+1}\leq\tau^{\sqrt{\frac{2l}{\tau-1}}}$. To choose τ we investigate the maximum value of the following function

$$f(\tau):=\tau^{\sqrt{\frac{2l}{\tau-1}}}=\exp\Big\{\sqrt{\frac{2l}{\tau-1}}\cdot\ln(\tau)\Big\},\quad 2\leq\tau\leq p-1.$$

Obviously, $f'(\tau)=\tau^{\sqrt{\frac{2l}{\tau-1}}}\cdot\Big(\frac{2l}{\tau-1}\Big)^{\frac{1}{2}}\cdot\Big(\frac{1}{\tau}-\frac{\ln\tau}{2(\tau-1)}\Big)$ and the function $f(\tau)$ reaches the maximum value at the point $\tau_0\in(4,92155,4,921555)$. Moreover, $f(\tau)$ monotonically decreases for $\tau\geq 5\geq\lceil\tau_0\rceil$, so $\mathfrak{d}_2=|\mathrm{T}|\geq 5^{\sqrt{l/2}}$.

(i) Let us show that $\mathfrak{d}_2\geq\mathfrak{u}(l-1,p-1)$ (see (3) and (P_2)). Indeed $ik+1<k(i+1)$, so

$$\sum_{i=0}^{l-1}(ki+1)u_i<k\sum_{i=0}^{l-1}(i+1)u_i<m,\tag{7}$$

and $\sum_{i=1}^{l}iu_{i-1}<\frac{m}{k}=l$.

If $u_{l-1}\neq 0$, we obtain a contradiction. Hence, $u_{l-1}=0$ and $\sum_{i=1}^{l-1}iu_{i-1}=l-1$, so $(u_0,\dots,u_{l-2})$ is a partition of $l-1$ (see (2)) such that $0\leq u_0,\dots,u_{l-2}\leq p-1$ and (7) holds.

Explicit lower bounds on $\mathfrak{q}(n_0,d_0)$ for $n\geq d_0^2$ and on $\mathfrak{u}(n_0)$ for all $n_0\in\mathbb{Z}$ are given in [8]. Note that $\mathfrak{u}(n_0,d_0-1)=\mathfrak{u}(n_0)$ for $n_0<d_0$. Using Lemmas 4 and 5 for $n_0:=l-1$ and $d_0:=p-1$ we obtain that

$$\begin{aligned}\mathfrak{d}_2\geq\mathfrak{u}(l-1,p-1)&=\mathfrak{q}(l-1,p)\\ &>\big(\frac{p(p-1)}{160(l-1)}\big)^{\sqrt{p}}\exp\Big(2.5\cdot\sqrt{(1-\tfrac{1}{p})(l-1)}\Big).\end{aligned}$$

(ii) Recall that if $n_0<d_0$, then $\mathfrak{u}(n_0,d_0-1)=\mathfrak{u}(n_0)$. Consequently

$$\mathfrak{d}_2\geq\mathfrak{u}(l-1,p-1)=\mathfrak{u}(l-1)>\frac{\exp\left(2.5\cdot\sqrt{l-1}\right)}{13(l-1)},$$

where $n_0=l-1$ and $d_0=p$ by Lemmas 5 and 6. □

Proof of Corollary 3. Elements $\theta^l + b, \theta + b \in F_q(\theta)$ are different and their orders are at least $\mathfrak{d}_1$ and $\mathfrak{d}_2$, respectively by Theorems 1 and 2.

If $k \leq \sqrt{l/2}$, then the order of $\theta + b$ has a lower bound $5^{\sqrt{l/2}}$ by Theorem 1. If $k > \sqrt{l/2}$, then we construct the element $\gamma = \theta^{m_2} + b$ with lower bound 5^k on its order by Theorem 2. Hence, one can explicitly construct in the field $F_q[x]/\langle x^m - a\rangle$ an element with the multiplicative order of at least $\max\{5^k, 5^{\sqrt{l/2}}\}$. In the worst case these lower bounds are equal $5^k = 5^{\sqrt{l/2}}$. Then $k = \sqrt[3]{m^2/2}$ and the order is at least $5^{\sqrt[3]{m/2}}$. □

Note that the two considered methods have two parts: the algebraic part and the combinatorial calculation. An improvement in either (or both) of these parts results in an improvement in the evaluation of the method and then in the approach. Generalizing the approach to other classes of finite fields is an open problem.

Acknowledgement

Authors would like to express their gratitude to an anonymous referee for valuable remarks and his/her help in improving this article. The research was supported by the UAEU UPAR grant G00003431.

References

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

[2] Andrews G.E. The theory of partitions. Encyclopedia of Mathematics and its Applications Vol. 2, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976.

[3] Berrizbeitia P. *Sharpening "PRIMES is in P" for a large family of numbers*. Math. Comp. 2005, **74** (252), 2043–2059. doi:10.1090/S0025-5718-05-01727-8

[4] 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

[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] von zur Gathen J., Shparlinski I. *Orders of Gauss periods in finite fields*. Appl. Algebra Engrg. Comm. Comput. 1998, **9** (1), 15–24. doi:10.1007/s002000050093

[7] Granville A. *It is easy to determine whether a given integer is prime*. Bull. Amer. Math. Soc. (N.S.) 2005, **42** (1), 3–38. doi:10.1090/S0273-0979-04-01037-7

[8] Maróti A. *On elementary lower bounds for the partition function*. Integers 2003, **3**, 1–9.

[9] Brochero M.F.E., Reis L. *Elements of high order in Artin-Schreier extensions of finite fields* $\mathbb{F}_q$. Finite Fields Appl. 2016, **41**, 24–33. doi:10.1016/j.ffa.2016.05.002

[10] Gary L. Mullen, Panario D. Handbook of finite fields. Discrete Mathematics and its Applications (Boca Raton). In: Mullen G. L., CRC Press, Boca Raton, FL, 2013. doi:10.1201/b15006

[11] Panario D., Thomson D. *Efficient pth root computations in finite fields of characteristic p*. Des. Codes Cryptogr. 2009, **50** (3), 351–358. doi:10.1007/s10623-008-9236-0

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

[13] 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

[14] Popovych R. *Sharpening of the explicit lower bounds for the order of elements in finite field extensions based on cyclotomic polynomials*. Ukrainian Math. J. 2014, **66** (6), 916–927. doi:10.1007/s11253-014-0981-0

[15] Popovych R. *On elements of high order in general finite fields*. Algebra Discrete Math. 2014, **18** (2), 295–300.

[16] Popovych R. *Lower bound on product of binomial coefficients*. Bul. Acad. Ştiinţe Repub. Mold. Mat. 2015, **2** (78), 21–26.

[17] Popovych R., Skuratovskii R. *Normal high order elements in finite field extensions based on the cyclotomic polynomials*. Algebra Discrete Math. 2020, **29** (2), 241–248. doi:10.12958/adm1117

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

Received 12.04.2022
Revised 29.04.2022

Бовді В., Діене А., Попович Р. *Елементи великого порядку в скінченних полях, заданих біномами* // Карпатські матем. публ. — 2022. — Т.14, №1. — С. 238–246.

Нехай F_q — скінченне поле з q елементів, де q є степенем простого числа $p \geq 5$. Поєднуючи два різних методи, для будь-якого цілого числа $m \geq 2$ і елемента $a \in F_q^*$ таких, що поліном $x^m - a$ є незвідним над $F_q[x]$, ми явно будуємо елементи великого порядку в полі $F_q[x]/\langle x^m - a\rangle$. А саме, знаходимо елементи з мультиплікативним порядком щонайменше $5\sqrt[3]{m/2}$, що краще, ніж отримана раніше оцінка для такої сім'ї розширень полів.

Ключові слова і фрази: скінченне поле, мультиплікативний порядок, елемент великого мультиплікативного порядку, біном.