ELEMENTS OF HIGH ORDER IN ARTIN-SCHREIER EXTENSIONS OF FINITE FIELDS $\mathbb{F}_q$

F. E. BROCHERO MARTÍNEZ AND LUCAS REIS

Abstract. In this article, we find a lower bound for the order of the coset $x + b$ in the Artin-Schreier extension $\mathbb{F}_q[x]/(x^p - x - a)$, where $b \in \mathbb{F}_q$ satisfies a generic special condition.

1. Introduction

For many important applications (for example, see [1]), it is interesting to find an element of very high order in a finite extension field $\mathbb{F}_q^n$. Ideally, one would choose a primitive element, but actually finding such an element is a notoriously hard computation problem. In fact, in order to verify that an element is primitive, we need to know the factorization of the integer $q^n - 1$ or to solve the discrete logarithms problem in $\mathbb{F}_q^n$. Now, with the tools currently known these two problems are very hard and they are the basis of modern cryptography.

On one hand, there are several methods used to find a small set of elements of $\mathbb{F}_q^n$ with at least one primitive element: In [13], assuming the extended Riemann hypothesis (ERH), Shoup has showed a deterministic polynomial-time search procedure in order to find a primitive element of $\mathbb{F}_{p^2}$; Also using ERH, Bach [3] gives an efficiently algorithm in order to construct a set of $O((\log p)^4/(\log \log p)^3)$ elements, that contain at least one generator of $\mathbb{F}_p^*$; In [7], Gao has given an algorithm to construct high order elements for almost all extensions $\mathbb{F}_{q^n}$ of finite fields $\mathbb{F}_q$, being the lower bound no less than $n \log q n^{4 \log_2 q} (2 \log q n)^-1$.

Chen [4] showed how to find, in polynomial time in $N$, an integer $n$ in the interval $[N, 2qN]$ and an element $\alpha \in \mathbb{F}_q^n$ with order greater than $\frac{5.8n}{\log q n}$.

On the order hand, many works have been done in order to find elements for which a reasonably large lower bound of the order can be guaranteed: Ahmadi, Shparlinski and Voloch [2] showed that if $\theta \in \mathbb{F}_{q^2}$ is a primitive $r$-th root of the unity, where $r = 2n + 1$ is a prime, then the Gauss period $\alpha = \theta + \theta^{-1}$ has order exceeding $\exp \left( \left( \pi \sqrt{\frac{2(a-1)}{3p}} + o(1) \right) \sqrt{n} \right)$, where $p$ is a characteristic of the field (for other works about the order of Gauss period, see [3, 9]). Popovych [8, 9] improved the previous bound and gave a lower bound for elements of the more general forms $\theta^e(\theta^f + a)$, $(\theta^{-f} + a)(\theta^f + a)$ and $\theta^{-2e}(\theta^{-f} + a)(\theta^f + a)^{-1}$, where $a \in \mathbb{F}_q^*$. In particular, he proved that the multiplicative order of the Gauss period $\beta = \theta + \theta^{-1}$ is not less than $5^{\sqrt{(r-2)/2}} - 2$, for all $p \geq 5$.

Date: February 19, 2016.

2010 Mathematics Subject Classification. 12E20 (primary) and 11T30 (secondary).

Key words and phrases. Multiplicative order, Gauss period, Artin-Schreier extensions.
Finally, Popovych [10] considered the Artin-Schreier extension $\mathbb{F}_{p^m}$ of finite field $\mathbb{F}_p$ and found that an element of order larger than $4^m$ by an elementary method. We emphasize that this Popovych’s result is weaker than the one, point out for Shparlinski in Voloch’s article [14], where, he say that the order of any root $t$ of $x^p - x - 1$ in $\mathbb{F}_{p^m}$ exceeds $2^{2.54p} \approx 5.81589^p$. Unfortunately, that article does not contain the proof of that limitation and making the computational calculations of that bound, using Sage Mathematics Software, we verify that it is true only in the case that $p > 4647$.

In this article, we consider the situation where $x^p - x - a$ is an irreducible polynomial of $\mathbb{F}_q[x]$, where $p$ is a characteristic of $\mathbb{F}_q$ and $a \in \mathbb{F}_p$. We find a lower bound for the multiplicative order of an element of the form $(\theta + b)$, where $\theta$ represents the coset of $x$ in the Artin-Schreier extension $\mathbb{F}_q[x]/(x^p - x - a)$ and $b$ satisfies an special condition. We also prove that, the probability that an element of $\mathbb{F}_q$ satisfies such special condition is close to 1 when $q$ is large enough.

Finally, in the case $q = p$, we show a lower bound which improves the result obtained by Popovych, but our lower bound does not reach the one appointed by Shparlinski-Voloch.

2. Preliminaries

Throughout this paper, $\mathbb{F}_q$ denotes a finite field of order $q$, where $q = p^n$ is a power of an odd prime $p$.

For each irreducible polynomial $f(x) \in \mathbb{F}_q[x]$, it is known that $\mathbb{F}_q[x]/(f)$ is a finite field with $q^n$ elements, where $d = \deg(f)$. Reciprocal, every vector field $\mathbb{F}_{q^d}$ is isomorphic to $\mathbb{F}_q[x]/(f)$ with $f$ an irreducible polynomial of degree $d$.

There are few known results to ensure the irreducibility of polynomials in a finite field. For example, Theorems 2.47 and 3.75 in [11] show the necessary and sufficient conditions for irreducibility of cyclotomic polynomials $\Phi_r(x)$ and binomials $x^t - a$, respectively. Other well-known result about the irreducibility of other family of polynomials is the following.

**Lemma 2.1.** The polynomial $x^p - x - a \in \mathbb{F}_q[x]$ is irreducible, if and only if, it has no roots in $\mathbb{F}_q$.

For the proof of this result, see (Theorem 3.78, [11]). In particular we have that

**Proposition 2.2.** Let $n$ be positive integer and $a \in \mathbb{F}_p^*$. The polynomial $f(x) = x^p - x - a$ is irreducible in $\mathbb{F}_q[x]$, if and only if, such that $p \nmid n$.

**Proof:** By Theorem 2.25 in [11], it is known that $a = b^p - b$, for some $b \in \mathbb{F}_q$, if and only if, $Tr_{\mathbb{F}_q/\mathbb{F}_p}(a) = a + a^p + \cdots + a^{p^{n-1}} \neq 0$. Since $a \in \mathbb{F}_p$, it follows that $Tr_{\mathbb{F}_q/\mathbb{F}_p}(a) = na$. But $Tr_{\mathbb{F}_q/\mathbb{F}_p}(a) \neq 0$, if and only if, $p$ does not divide $n$. \qed

The main results of this paper is the following one:

**Theorem 2.3.** Let $x^p - x - a$ be an irreducible polynomial of $\mathbb{F}_q$, with $q = p^n$ $(n \geq 2)$ and $a \in \mathbb{F}_p$. If $\theta$ is the coset of $x$ in the Artin-Schreier extension $\mathbb{F}_q[x]/(x^p - x - a)$ and $b \in \mathbb{F}_q$ satisfies that $b \notin \mathbb{F}_{p^m}$, for all $m$ proper divisor of $n$, then the multiplicative order of $\theta + b$ is lower bounded by

$$
\frac{1}{\pi(p-1)} \sqrt{\frac{2n+1}{2n-1}} \left( \frac{(2n+1)^{2n+1}}{(2n-1)^{2n-1}} \right)^{(p-1)/2} \exp \left( -\frac{1}{3(p-1)} \left( \frac{4n^2}{4n^2 - 1} \right) \right).
$$
In particular, for every \( \epsilon > 0 \) and \( n > N_\epsilon \),
\[
|\langle \theta + b \rangle| > \frac{1}{\pi p} ((e - \epsilon)(2n + 1))^{p-1}.
\]

And for the case \( p = q \), i.e., \( n = 1 \), we obtain

**Theorem 2.4.** Let \( a \neq 0 \) and \( b \) be arbitrary elements of \( \mathbb{F}_p \). Then the multiplicative order of \( (\theta + b) \) in \( \frac{F_p[x]}{(x^p - x - a)} \) is lower bounded by \( \frac{\sqrt[p]{3}}{p} e^{-\frac{1}{2}} (\frac{16}{p})^p \).

Observe that using the fields isomorphism
\[
\tau : \frac{F_q[x]}{(x^p - x - a)} \rightarrow \frac{F_q[x]}{(x^p - x - 1)}
\]
we only need to prove the Theorem in the case \( a = 1 \).

3. The finite field \( \mathbb{F}_q[x]/(x^p - x - 1) \)

Throughout this section, \( x^p - x - 1 \) is an irreducible polynomial of \( \mathbb{F}_q[x] \), where \( q = p^n \), \( \gcd(p,n) = 1 \). Also, \( \theta \) represents the coset of \( x \) in the Artin-Schreier extensions \( K := \mathbb{F}_q[x]/(x^p - x - 1) \) and \( b \in \mathbb{F}_q \setminus \mathcal{A}_n \), where
\[
\mathcal{A}_n = \bigcup_{m|n} \mathbb{F}_{p^m}.
\]

Before we estimate the order of \( \theta + b \), let us show that almost all element of \( \mathbb{F}_q \) satisfies the condition that we are imposing on \( b \).

**Theorem 3.1.** The number of elements of \( \mathbb{F}_q \setminus \mathcal{A}_n \) is \( \sum_{d|n} p^d \mu(n/d) \), where \( \mu \) is the Möbius function. In particular, the probability that a chosen element in \( \mathbb{F}_q \) does not belong to \( \mathcal{A}_n \) is greater than \( 1 - \frac{\log n}{q^{1/2}} \), where \( r \) is the smallest prime divisor of \( n \).

**Proof:** For each positive integer \( m \), let \( g : \mathbb{N}^* \rightarrow \mathbb{N} \) be the function defined by
\[
g(m) = |\mathbb{F}_{p^m} \setminus \mathcal{A}_m|.
\]

Clearly, for each positive integer \( m \), \( g(m) \) counts the number of elements in \( \mathbb{F}_{p^m} \), which are not in any proper subfield of \( \mathbb{F}_{p^m} \). Since each proper field is of the form \( \mathbb{F}_{p^l} \), where \( l|m \), then
\[
\sum_{d|m} g(d) = |\mathbb{F}_{p^m}| = p^m.
\]

By the Möbius Inversion Formula, it follows that
\[
g(m) = \sum_{d|m} p^d \mu(m/d).
\]

Now, let us calculate an upper bound for the number of elements in \( \mathcal{A}_n \). Let us suppose that \( \prod_{i=1}^{s} p_i^{n_i} \) is the factorization of \( n \) in prime factors, where \( p_1 < \cdots < p_s \). For each proper divisor \( d \) of \( n \), there exists a prime \( p_i \) (\( 1 \leq i \leq s \)), such that \( d|/(n/p_i) \). Thus \( \mathcal{A}_n \subset \bigcup_{1 \leq i \leq s} \mathbb{F}_{p_i^{n_i}} \), where \( n_i = \frac{n}{p_i} \). In particular
\[
|\mathcal{A}_n| \leq \bigcup_{1 \leq i \leq s} \mathbb{F}_{p_i^{n_i}} \leq \sum_{1 \leq i \leq s} p_i^{n_i} \leq p^{n/p_1} \log p_1, n = q^{1/p_1} \log p_1, n.
\]
Therefore, the probability that a chosen element in \( \mathbb{F}_q \) does not belong to \( A_n \) is greater than
\[
1 - \frac{|A_n|}{q} = 1 - \frac{\log_{p^i}(n)}{q(1-1/p)}.
\]

This theorem proves that almost all element in \( \mathbb{F}_q \) satisfies the condition that we imposed on \( b \). Now, we need the following technical lemmas:

**Lemma 3.2.** Let \( i \) and \( j \) be integers such that \( 0 \leq i, j \leq np - 1 \). If \( i \neq j \), then \( i + b^{p^i} \neq j + b^{p^j} \).

**Proof:** Let \( i_0 \) (respectively \( j_0 \)) be the remainder of \( i \) (respectively \( j \)) divided by \( n \). We can suppose, without loss of generality, that \( i_0 \geq j_0 \). Clearly, \( b^{p^i} = b^{p^{i_0}} \) and \( b^{p^j} = b^{p^{j_0}} \). Now suppose, by contradiction, that \( i + b^{p^i} = j + b^{p^j} \) and therefore
\[
(j - i) = b^{p^{i_0}} - b^{p^{j_0}}.
\]

In the case when \( i_0 = j_0 \), we have that \( j \equiv i \pmod{n} \), i.e., \( j = i + nk \) for some integer \( k \) and
\[
0 = b^{p^j} - b^{p^i} = i - j = nk.
\]

It follows that \( p \) divides \( k \), what is impossible because \( 0 < |i - j| < np \).

Thus \( 0 < i_0 - j_0 < n \), and taking the \( p^{n-j_0} \)-th power in (2), we have
\[
j - i = b^{p^{i_0}} - b^{p^{j_0}} - b = b^{p^{i_0}} - b.
\]

Thereby, there exists \( 0 \leq t < n \) such that \( b^{p^t} - b \in \mathbb{F}_p \), or equivalently \( b^{p^{t+1}} - b = (b^{p^t} - b)p = b^{p^t} - b \). This last equation can be rewritten as \( b^p - b = (b^p - b)p^t \), i.e., \( b^p - b \) is an element of \( \mathbb{F}_p \). Furthermore, if \( b \notin \mathbb{F}_p \), by Lemma 2.1 the polynomial \( x^p - x - (b^p - b) \) is an irreducible polynomial of \( \mathbb{F}_p \). We obtain, in any case, that \( b \in \mathbb{F}_p^* \). Since \( b \) is also in \( \mathbb{F}_{p^n} \), we conclude that \( b \) belongs to
\[
\mathbb{F}_{p^n} \cap \mathbb{F}_p^* = \mathbb{F}_{p^\gcd(p,n)} = \mathbb{F}_{p^\gcd(t,n)},
\]
where \( \gcd(t,n) < n \) is a proper divisor of \( n \) and so we have a contradiction with the choice of \( b \notin A_n \).

**Lemma 3.3.** Let \( t, s \) be nonnegative integers such that \( 0 \leq t + s \leq p - 1 \) and let \( I_{s,t} \) be the subset of \( \mathbb{Z}^{np} \) such that \( \vec{r} := (r_0, r_1, \ldots, r_{np-1}) \in I_{s,t} \) if and only if
\[
\sum_{0 \leq j \leq np-1 \atop r_j < 0} (-r_j) \leq t \quad \text{and} \quad \sum_{0 \leq j \leq np-1 \atop r_j \geq 0} r_j \leq s.
\]

Then the function
\[
\Lambda : I_{s,t} \rightarrow G,
\]
\[
\vec{r} \mapsto \prod_{0 \leq j \leq np-1} (\theta + b)^{r_j p^j},
\]
where \( G = (\theta + b) \leq \mathbb{K}^* \), is one to one.

**Proof:** Since \( \theta \) is the coset of \( x \) in the quotient field \( \mathbb{K} = \mathbb{F}_p[x] / (x^{p^t} - x - 1) \), then each element of \( \mathbb{K} \) is the coset of a unique \( h(\theta) \), where \( h \) is a polynomial in \( \mathbb{F}_p[x] \) of degree at most \( p - 1 \). In addition, \( \theta^{p^j} = \theta + 1 \) and, accordingly, for all \( j \in \mathbb{N} \),
\[
\theta^{p^{j+1}} = (\theta^p)^{p^j} = (\theta + 1)^{p^j} = \theta^{p^j} + 1.
\]
It follows, inductively, that 
\[ \theta^{p^j} = \theta + j \quad \text{for all } j \geq 1, \]
and, thereby, for each \( \vec{r} = (r_0, \ldots, r_{np-1}) \in I_{s,t} \)
\[ \Lambda(\vec{r}) = \prod_{0 \leq i \leq np-1} (\theta + b)^{r_ip^i} = \prod_{0 \leq i \leq np-1} (\theta + i + b^{p^j})^{r_i}. \]

Now, suppose that \( \vec{s} = (s_0, \ldots, s_{np-1}) \) is another element of \( I_{s,t} \) such that \( \Lambda(D) = \Lambda(E) \), i.e.,
\[ \prod_{0 \leq i \leq np-1} (\theta + i + b^{p^j})^{r_i} = \prod_{0 \leq j \leq np-1} (\theta + j + b^{p^j})^{s_j}, \]
thus, the polynomial
\[ F(x) = \prod_{0 \leq i \leq np-1} (x + i + b^{p^j})^{r_i} \prod_{0 \leq j \leq np-1} (x + j + b^{p^j})^{-s_j} \]
is congruent to the polynomial
\[ G(x) = \prod_{0 \leq j \leq np-1} (x + j + b^{p^j})^{s_j} \prod_{0 \leq i \leq np-1} (x + i + b^{p^j})^{-r_i} \]
modulo \( x^p - x - 1 \).
Since \( \deg(F) \leq s + t \leq p - 1 \) and \( \deg(G) \leq s + t < p - 1 \), it follows that \( F(x) = G(x) \). Further, by Lemma 3.2, we know that \( x + i + b^{p^j} \neq x + j + b^{p^j} \), for all \( 0 \leq i < j \leq np-1 \), therefore \( \vec{r} = \vec{s} \), as we want to prove. \( \square \)

We emphasize that, in the last step of Lemma, is essential the condition that we imposed on \( b \).

**Lemma 3.4.** Let \( I_{s,t} \) be as in the Lemma 3.3. Then

\[ |I_{s,t}| = \sum_{j=0}^{t} \sum_{i=0}^{s} \binom{np-i}{i} \binom{np-j}{j} \binom{s}{i} \binom{t}{j}. \]
In particular,
\[ |I_{s,t}| > \binom{np+t-s}{t} \binom{np+s}{s}. \]

**Proof:** Observe that, for each \( j \leq t \) and \( i \leq s \), we can select \( j \) coordinates of \( \vec{r} \) to be negative and \( i \) coordinates to be positive and this choice can be done of \( \binom{np-i}{i} \binom{np-j}{j} \binom{s}{i} \binom{t}{j} \) ways. Besides, the number of positive solution of \( x_1 + x_2 + \cdots + x_i \leq s \) is \( \binom{s}{i} \) and the number of positive solution of \( x_1 + x_2 + \cdots + x_j \leq t \) is \( \binom{t}{j} \). Thus, for each pair \( i, j \), there exist \( \binom{np-i}{i} \binom{np-j}{j} \binom{s}{i} \binom{t}{j} \) elements of \( I_{s,t} \) and then, adding over all
\[ |I_{s,t}| \geq \sum_{i=0}^{s} \binom{s}{i} (np)^i \left( \sum_{j=0}^{t} \binom{np-i}{j} t^j \right) \]
\[ = \sum_{i=0}^{s} \frac{s}{i} \binom{np+t-i}{t} \]
\[ > \binom{np+t-s}{t} \sum_{i=0}^{r} \frac{s}{i} \binom{np}{i} \]
\[ = \binom{np+t-s}{t} \binom{np+s}{s} \]

Before proceeding to prove the main Theorems, we need the following technical Lemma, that is essentially a good application of Stirling approximation.

**Lemma 3.5** ([12] Corollary 1). For all \( s > 0 \) and \( r > 1 \), we have
\[
c_r \cdot d_r^s \cdot \frac{1}{\sqrt{s}} \cdot \Theta(r, s) < \binom{rs}{s} < c_r \cdot d_r^s \cdot \frac{1}{\sqrt{s}},
\]
where
\[ c_r = \sqrt{\frac{r}{2\pi(r-1)}}, \quad d_r = \frac{r^r}{(r-1)^{r-1}} \]
and
\[ \Theta(r, s) = \exp \left( -\frac{1}{12s} \left( 1 + \frac{1}{r(r-1)} \right) \right). \]

We emphasize that these upper and lower bounded are very close when \( s \gg 0 \).

### 4. Proof of Theorem 2.3

By Lemma 3.3, we know that \(|\langle \theta + b \rangle| \geq |I_{s,t}|\), for all nonnegative integers \( s \) and \( t \) such that \( s + t \leq p - 1 \). So, by Lemma 3.3, we have that
\[
|\langle \theta + b \rangle| > \max_{0 \leq s+t \leq p-1} \binom{np+t-s}{t} \binom{np+s}{s}
\]
\[ > \binom{np}{(p-1)/2} \binom{np+(p-1)/2}{(p-1)/2}. \]

(4)

Now, using Lemma 3.5, each binomial coefficient can be bounded by
\[ \binom{np}{(p-1)/2} > \binom{(2n)(p-1)/2}{(p-1)/2} \]
\[ > \sqrt{\frac{2n}{\pi(2n-1)(p-1)}} \left( \frac{(2n)^{2n}}{(2n-1)^{2n-1}} \right)^{\frac{p-1}{2}} \Theta(2n-1) \]
and
\[ \binom{np+(p-1)/2}{(p-1)/2} > \binom{(2n+1)(p-1)/2}{(p-1)/2} \]
\[ > \sqrt{\frac{2n+1}{\pi(2n)(p-1)}} \left( \frac{(2n+1)^{2n+1}}{(2n)^{2n}} \right)^{\frac{p-1}{2}} \Theta(2n+1) \]
where $\tilde{\Theta}(z) = \exp \left( -\frac{1}{6(p-1)} \left( 1 + \frac{1}{z(z-1)} \right) \right)$.

Multiplying these two inequalities and simplifying, we conclude that

$$|\langle \theta + b \rangle| > \frac{1}{\pi(p-1)} \sqrt{\frac{2n+1}{2n-1}} \left( \frac{(2n+1)^{2n+1}}{(2n-1)^{2n-1}} \right)^{(p-1)/2} \exp \left( -\frac{1}{3(p-1)} \left( \frac{4n^2}{4n^2-1} \right) \right).$$

Therefore, we obtain the first part of the Theorem.

For the second part, observe that the sequence $\{a_n\}_{n\in\mathbb{N}}$ defined for each $n \geq 2$, as $a_n := \left( \frac{2n+1}{2n-1} \right)^{(p-1)/2}$, is an increasing sequence satisfying

$$a_2 > \sqrt[3]{\frac{5}{3}}(2.1516)^{p-1} \quad \text{and} \quad \lim_{n \to \infty} a_n = e^{p-1}.$$ 

Therefore, for $n \geq 2$, we can find a simpler but weaker estimate

$$|\langle \theta + b \rangle| > \frac{1}{\pi(p-1)} (a_n(2n+1))^{p-1} \exp \left( -\frac{1}{3(p-1)} \left( \frac{4n^2}{4n^2-1} \right) \right)$$

$$> \frac{\sqrt[3]{5}}{\sqrt{3\pi(p-1)}}(2.1516(2n+1))^{p-1} \exp \left( -\frac{16}{45(p-1)} \right).$$

In the case $n$ large enough, we have that

$$(e - \epsilon)^{p-1} < a_n < e^{p-1} \quad \text{and} \quad \exp \left( -\frac{1}{3(p-1)} \left( \frac{4n^2}{4n^2-1} \right) \right) > 1 - \frac{16}{45(p-1)},$$

therefore

$$|\langle \theta + b \rangle| > \frac{45p - 61}{45\pi(p-1)^2} ((e - \epsilon)(2n+1))^{p-1}$$

$$> \frac{1}{\pi p} ((e - \epsilon)(2n+1))^{p-1},$$

as we want to prove. \(\square\)

The following table the lower bounded of $|\langle \theta + b \rangle|$, for some values of $n$, where the value of $p$ appears as a parameter

| $n$  | $\pi p \cdot |\langle \theta + b \rangle|$ |
|------|----------------------------------|
| 2    | 12.22377$^p$                     |
| 3    | 17.65835$^p$                     |
| 4    | 23.09586$^p$                     |
| 5    | 28.53356$^p$                     |
| 10   | 55.71983$^p$                     |
| 100  | 545.01494$^p$                    |
| 1000 | 5437.92274$^p$                   |
| 10000| 54366.9957$^p$                   |
5. Proof of Theorem 2.4

The polynomial \( x^p - x - 1 \) is always an irreducible polynomial of \( \mathbb{F}_p[x] \) and the condition imposed on \( b \) is empty. So, by Lemma 3.4, we have that

\[
|\langle \theta + b \rangle| > \max_{s+t=p-1} \left( \frac{p+t-s}{t} \right) \left( \frac{p+s}{s} \right).
\]

\[
= \max_{0 \leq s \leq p-1} \left( \frac{2p - 1 - 2s}{p - 1 - s} \right) \left( \frac{p + s}{s} \right).
\]

\[
= \max_{0 \leq \lambda \leq p-1} \left( \frac{2p - 1 - 2p\lambda}{p - 1 - p\lambda} \right) \left( \frac{p + p\lambda}{p\lambda} \right).
\]

\[
= \frac{1}{2} \max_{0 \leq \lambda \leq p-1} \left( \frac{p(2 - 2\lambda)}{p(1 - \lambda)} \right) \left( \frac{p(1 + \lambda)}{p\lambda} \right).
\]

The same way, using Lemma 3.5, we obtain that

\[
|\langle \theta + b \rangle| > \max_{0 \leq \lambda \leq p-1} \frac{1}{\pi p} \sqrt{\frac{1 + \lambda}{2\lambda(1 - \lambda)}} \left( \frac{4^{1-\lambda}(1 + \lambda)^{1+\lambda}}{\lambda^\lambda} \right)^p \Theta(2, p(1-\lambda)) \Theta \left( \frac{1 + \lambda}{\lambda}, p\lambda \right),
\]

in particular, taking \( \lambda = \frac{1}{3} \), it follows that

\[
|\langle \theta + b \rangle| > \frac{\sqrt{3}}{\pi p} e^{-\frac{1}{2p}} \left( \frac{16}{3} \right)^p.
\]

\[\square\]

Remark 5.1. In summary, for the case \( \mathbb{F}_p \) and \( p \gg 0 \), we observe that lower bound of \( |\langle \theta + b \rangle| \) is \( O(4^p) \) in Popovych’s paper, \( O(5.81589^p) \) in Voloch’s article and \( O(5.3333^p) \) in our result.

References

[1] Agrawal, M., Kayal, N., Saxena, N., Primes is in P, Ann. of Math., 160 (2004), 781-793.
[2] Ahmadi, O., Shparlinski, I., Voloch, J. F., Multiplicative order of Gauss periods. Int. J. Number Theory 6 (2010), 877-882.
[3] Bach, E., Comments on search procedures for primitive roots. Math. Comp. 66 (1997), no. 220, 1719-1727
[4] Cheng, Q., Constructing finite field extensions with large order elements. SIAM J. Discrete Math. 21 (2007), 726-730.
[5] Gathen, J. and Shparlinski, I.E., Orders of Gauss periods in finite fields, Appl. Algebra in Engin., Commun. and Compo 9 (1998), 15-24
[6] Gathen, J. and Shparlinski, I.E., Constructing elements of large order in finite fields. Applied algebra, algebraic algorithms and error-correcting codes. Lecture Notes in Comput. Sci., 1719 (1999), 404-409.
[7] Gao, S., Elements of provable high orders in finite fields. Proc. Amer. Math. Soc. 127 (1999), 1615-1623.
[8] Popovych, R., Elements of high order in finite fields of the form \( \mathbb{F}_q[x]/\Phi_r(x) \). Finite Fields Appl. 18 (2012), 700-710.
[9] Popovych, R., Sharpening of the explicit lower bounds for the order of elements in finite field extensions based on cyclotomic polynomials. Ukrainian Math. J. 66 (2014), 916-927
[10] Popovych, R., Elements of high order in Artin-Shreier extensions of finite fields. Mat. Stud. 39 (2013), 115-118
[11] Lidl, R., Niederreiter, H., Finite Fields. Encyclopedia of Mathematics and Its Applications, Vol 20, Addison-Wesley 1983.
[12] Sasvári, Z., Inequalities for binomial coefficients. J. Math. Anal. Appl. 236 (1999), 223-226.
[13] Shoup, V. Searching for primitive roots in finite fields. Math. Comp. 58 (1992), no. 197, 369-380

[14] Voloch, J. F., On some subgroups of the multiplicative group of finite rings. J. Théor. Nombres Bordeaux 16 (2004), 233-239.

Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 30123-970, Brazil,
E-mail address: fbrocher@mat.ufmg.br
E-mail address: lucasreismat@gmail.com