Incomplete exponential sums over exponential functions

Bryce Kerr
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
bryce.kerr@mq.edu.au

Abstract
We extend some methods of bounding exponential sums of the type

\[ \sum_{n \leq N} e^{2\pi i \alpha n / p} \]

to deal with the case when \( \alpha \) is not necessarily a primitive root. We also show some recent results of Shkredov concerning additive properties of multiplicative subgroups imply new bounds for the sums under consideration.

1 Introduction
For \( p \) prime, \( g \in \mathbb{F}_p^* \) of order \( t \) and integer \( N \leq t \) we consider the sums

\[ S_{g,p}(\lambda, N) = \sum_{n=1}^{N} e_p(\lambda g^n) \]  

where \( e_p(z) = e^{2\pi iz / p} \) and \( \gcd(\lambda, p) = 1 \). Estimates for \( S_{g,p}(\lambda, N) \) have been considered in a number of works. For instance Korobov \([7]\) obtains the bound

\[ \max_{\gcd(\lambda,p)=1} |S_{g,p}(\lambda, N)| \ll p^{1/2} \log p \]  

which is used to study the distribution of digits in decimal expansions of rational numbers (see also \([10]\) and references therein). If \( g \) is a primitive root, Bourgain and Garaev \([11]\) give bounds for the number of solutions to the equation

\[ g^{x_1} + g^{x_2} \equiv g^{x_3} + g^{x_4} \pmod{p}, \quad 1 \leq x_1, \ldots, x_4 \leq N, \]
which they use to estimate $S_{g,p}(\lambda, N)$. Konyagin and Shparlinski \cite{6} improve on this bound and give applications to the gaps between powers of a primitive root.

The case of complete sums with $N = t$ have also been considered by a number of authors (see for example \cite{5}) from which corresponding bounds for the incomplete sums can be obtained using a method of \cite{9}.

We show that the proof of \cite{1} Theorem 1.4] can be generalized to deal with the case when $g$ is not a primitive root. This gives an upper bound for the sums

$$\sum_{\lambda \in \mathbb{F}_p^*} |S_{g,p}(\lambda, N)|^4. \quad (3)$$

We then combine the argument of \cite{6} Theorem 1] and our upper bound for (3) to deduce a bound for $S_{g,p}(\lambda, N)$. Next we show that \cite{9} Theorem 34] combined with a method of \cite{9} gives another bound for $S_{g,p}(\lambda, N)$.

We use the notation $f(x) \ll g(x)$ and $f(x) = O(g(x))$ to mean there exists some absolute constant $C$ such that $f(x) \leq C g(x)$ and $f(x) = o(g(x))$ will mean that $f(x) \leq \varepsilon g(x)$ for any $\varepsilon > 0$ and sufficiently large $x$.

2 Main results

**Theorem 1.** For prime $p$ and $g \in \mathbb{F}_p^*$ of order $t$ and integer $N \leq t$, we have

$$\sum_{\lambda \in \mathbb{F}_p^*} |S_{g,p}(\lambda, N)|^4 \ll pN^{71/24+o(1)} (1 + (N^2/t)^{1/24})$$

as $N \to \infty$.

We use Theorem \cite{11} to deduce

**Theorem 2.** For $g \in \mathbb{F}_p^*$ of order $t$ and integer $N \leq t$, we have

$$\max_{\gcd(\lambda,p)=1} |S_{g,p}(\lambda, N)| \leq \begin{cases} p^{1/8} N^{71/96+o(1)}, & N \leq t^{1/2}, \\ p^{1/8} t^{-1/96} N^{49/96+o(1)}, & t^{1/2} < N \leq p^{1/2}, \\ p^{1/4} t^{-1/96} N^{49/96+o(1)}, & p^{1/2} < N < t, \end{cases}$$

as $N \to \infty$.

The following is a consequence of \cite{7} Lemma 2] and \cite{8} Theorem 34]

**Theorem 3.** For $g \in \mathbb{F}_p^*$ of order $t$ and integer $N \leq t$, we have

$$\max_{\gcd(\lambda,p)=1} |S_{g,p}(\lambda, N)| \ll \begin{cases} p^{1/8} t^{22/36} (\log p)^{7/6}, & t \leq p^{1/2}, \\ p^{1/4} t^{13/36} (\log p)^{7/6}, & p^{1/2} < t \leq p^{3/5} (\log p)^{-6/5}, \\ p^{1/6} t^{1/2} (\log p)^{4/3}, & p^{3/5} < t \leq p^{2/3} (\log p)^{-2/3}, \\ p^{1/2} \log p, & t > p^{2/3} (\log p)^{-2/3}. \end{cases}$$
We may combine Theorem 2 and Theorem 3 into a single result for particular values of $t$. For instance, when $t$ has order $p^{1/2}$ we get

**Corollary 4.** Suppose $g \in \mathbb{F}^*_p$ has order $t$ with $p^{1/2} \ll t \ll p^{1/2}$. Then

$$\max_{\gcd(\lambda, p) = 1} |S_{\lambda, g, p}(N)| \leq \begin{cases} p^{1/8 + o(1)} N^{71/96}, & N \leq p^{1/4}, \\ p^{23/192 + o(1)} N^{73/96}, & p^{1/4} < N \leq p^{179/438}, \\ p^{31/72 + o(1)}, & p^{179/438} < N \ll p^{1/2}. \end{cases}$$

## 3 Preliminary Results

Given $A, B \subseteq \mathbb{F}_p$, we define

$$A + B = \{ a + b : a \in A, b \in B \}$$

and

$$A \backslash B = \{ ab^{-1} : a \in A, b \in B, b \neq 0 \}.$$  

We follow the method of [1] to generalise [1, Lemma 2.8]

**Lemma 5.** Suppose $g \in \mathbb{F}^*_p$ has multiplicative order $t$ and let $L_1, L_2, M$ be non-negative integers with $1 \leq M \leq t$. Let

$$\mathcal{X} \subseteq [L_1 + 1, L_1 + M] \quad \text{and} \quad \mathcal{Y} \subseteq [L_2 + 1, L_2 + M]$$

be two sets of integers of cardinalities

$$\# \mathcal{X} = M \Delta_1 \quad \text{and} \quad \# \mathcal{Y} = M \Delta_2.$$

Then for the sets

$$A = \{ g^x : x \in \mathcal{X} \} \quad \text{and} \quad B = \{ g^y : y \in \mathcal{Y} \}$$

we have

$$\#(A + B) \geq \min \left\{ M^{9/8 + o(1)} \Delta_1^{3/4} \Delta_2, t^{1/8} M^{7/8 + o(1)} \Delta_1^{5/8} \Delta_2 \right\}.$$  

**Proof.** We follow the proof of [1, Lemma 2.8] and begin by considering the sum

$$\sum_{a_1, a_2 \in A} \#(a_1 B \cap a_2 B) = \#\{(a_1, a_2, b_1, b_2) \in A \times A \times B \times B : a_1 b_1 = a_2 b_2\}.$$
By [11] Lemma 2.9] and the Cauchy-Schwarz inequality we get
\[ \sum_{a_1, a_2 \in A} \# (a_1 B \cap a_2 B) \geq \frac{(\# A)^2 (\# B)^2}{\# (AB)} \]
hence there exists some fixed \( a_0 \in A \) such that
\[ \sum_{a \in A} \# (a B \cap a_0 B) \geq \frac{\# A (\# B)^2}{\# (AB)}. \]

Using an argument from [2, Theorem 1], for positive integer \( j \leq \log \# B / \log 2 + 1 \), let \( D_j \) be the set of all \( a \in A \) such that
\[ 2^{j-1} \leq \# (a B \cap a_0 B) < 2^j \]
and set \( D_j = \emptyset \) otherwise. Then we have
\[ \sum_j \sum_{a \in D_j} 2^j \geq \sum_{a \in A} \# (a B \cap a_0 B) \geq \frac{\# A (\# B)^2}{\# (AB)}. \]

We choose \( j_0 \) so that \( \sum_{a \in D_{j_0}} 2^j \) is maximum for \( j = j_0 \) and let
\[ N = 2^{j_0-1}, \quad A_1 = D_{j_0} \subseteq A, \]
so that
\[ N \leq \# (a B \cap a_0 B) \leq 2N. \]

We have
\[ (\log \# B / \log 2 + 1) \sum_{a \in D_{j_0}} 2^{j_0-1} \geq \sum_j \sum_{a \in D_j} 2^j \geq \frac{\# A (\# B)^2}{\# (AB)} \]
and the inequality \( \# B \leq M \) gives
\[ N \# A_1 \geq \frac{\# A (\# B)^2}{4 \# (AB) \log M}. \]

Since \( 1 \leq M \leq t \), for any \( x_1, x_2 \in \mathcal{X} \) we have \( x_1 \not\equiv x_2 \pmod{t} \) so that \( g^{x_1} \not\equiv g^{x_2} \pmod{p} \), hence we get
\[ \# A = M \Delta_1, \quad \# B = M \Delta_2, \]
and
\[ \# (AB) = \# \{ g^{x+y} : x \in \mathcal{X}, y \in \mathcal{Y} \} \ll M. \]
Inserting (7), (8), (9) into (6) and recalling that $N \leq \#B$ and $\#A_1 \leq \#A$ gives

$$N \#A_1 \gg M^2 \frac{\Delta_1 \Delta_2}{\log M}, \quad (10)$$

$$\#A_1 \gg M \frac{\Delta_1 \Delta_2}{\log M}, \quad (11)$$

$$N \gg M \frac{\Delta_2^2}{\log M}. \quad (12)$$

By [1, Lemma 2.6] we have

$$\#(aA \pm a_0A) \leq \frac{(\#(A + B))^2}{\#(aB \cap a_0B)} \leq \frac{(\#(A + B))^2}{\#(aB \cap a_0B)},$$

so that for any $a \in A_1$, by (5)

$$\#(aA \pm a_0A) \leq \frac{(\#(A + B))^2}{N}. \quad (13)$$

Using the same argument from the beginning of the proof, there exists $a'_0 \in A_1$ such that

$$\sum_{a \in A_1} \#(aA_1 \cap a'_0A_1) \geq \frac{(\#A_1)^3}{\#(A_1A_1)}. \quad (14)$$

Let $A_2$ be the set of all $a \in A_1$ such that

$$\#((a/a'_0)A_1 \cap A_1) \geq \frac{(\#A_1)^2}{2\#(A_1A_1)}. \quad (15)$$

Then we have

$$\#A_2 \geq \frac{(\#A_1)^2}{2\#(A_1A_1)}, \quad (16)$$

since if the inequality (16) were false, we would have

$$\sum_{a \in A_1} \#(aA_1 \cap a'_0A_1) = \sum_{a \in A_2} \#(aA_1 \cap a'_0A_1) + \sum_{a \in A_1 \setminus A_2} \#(aA_1 \cap a'_0A_1)$$

$$\leq \#A_2 \#A_1 + \#A_1 \frac{(\#A_1)^2}{2\#(A_1A_1)}$$

$$< \frac{(\#A_1)^3}{\#(A_1A_1)} \left( \frac{1}{2} + \frac{1}{2} \right) = \frac{(\#A_1)^3}{\#(A_1A_1)},$$

5
which contradicts (14). Let
\[ d_0 = \max\{ \text{ord}_p (a/a'_0) : a \in \mathcal{A}_2 \} = \text{ord}_p (a''_0/a'_0) \]
for some \( a''_0 \in \mathcal{A}_2 \). We split the remaining proof into 2 cases:

**Case 1:**
\[ \# \left( \frac{\mathcal{A}_1 - \mathcal{A}_1}{\mathcal{A}_1} \right) < \text{ord}_p (a''_0/a'_0) \]

Let
\[ C = (a''_0/a_0) \mathcal{A}_1 \cap \mathcal{A}_1 \]
then we have
\[ \# \left( \frac{C - C}{\mathcal{A}_1} \right) \leq \# \left( \frac{\mathcal{A}_1 - \mathcal{A}_1}{\mathcal{A}_1} \right) < \text{ord}_p (a''_0/a'_0) \] (17)
so there exists \( c_1, c_2 \in C \) and \( a_3, a_4 \in \mathcal{A}_1 \) such that
\[ (a'_0/a''_0)^{c_1} c_2 \neq \frac{C - C}{\mathcal{A}_1} \]
Since if \( (a'_0/a''_0)y \in \frac{C - C}{\mathcal{A}_1} \), then the distinct elements
\[ y, (a'_0/a''_0)y, \ldots, (a'_0/a''_0)^{\text{ord}_p (a''_0/a'_0) - 1}y \]
all belong to \( \frac{C - C}{\mathcal{A}_1} \), contradicting (17). Using a similar argument, we may show that we have strict subset inclusion \( C \subset \mathcal{A}_1 \) so that we may choose \( a_1, a_2 \in \mathcal{A}_1 \) such that
\[ \frac{a_1 - a_2}{a_3 - a_4} \neq \frac{C - C}{\mathcal{A}_1} \]
Hence by [3, Lemma 3.1] we have
\[ \#((a_1 - a_2) \mathcal{A} + (a_3 - a_4) \mathcal{A}) \geq \# \left( \mathcal{C} + \frac{a_1 - a_2}{a_3 - a_4} \mathcal{A}_1 \right) \geq \# \mathcal{A}_1 \# \mathcal{C} \]
and since \( a''_0 \in \mathcal{A}_2 \), we have by (15)
\[ \#((a_1 - a_2) \mathcal{A} + (a_3 - a_4) \mathcal{A}) \geq \frac{(# \mathcal{A}_1)^3}{# (\mathcal{A}_1 \mathcal{A}_1)} \] (18)
In [1] Lemma 2.7] we take \( k = 4 \) and
\[ B_1 = a_1 \mathcal{A}, \quad B_2 = -a_2 \mathcal{A}, \quad B_3 = a_3 \mathcal{A}, \quad B_4 = -a_4 \mathcal{A}, \quad X = a_0 \mathcal{A}, \]
which gives
\[
\#(a_1A - a_2A + a_3A - a_4A) \leq \frac{\#(a_0A + a_1A)\#(a_0A - a_2A)\#(a_0A + a_3A)\#(a_0A - a_4A)}{(#A)^3}.
\] (19)

The inequality \((a_1 - a_2)A + (a_3 - a_4)A \leq (a_1A - a_2A + a_3A - a_4A)\) along with (13) and (18) gives
\[
(#(A + B))^8 \geq \frac{((#A_1)^3(#A_4)^3N^4}{(#A_1A_4)}.
\]

Inserting (7), (10) and (12) into the above and using \(#(A_1A_4) \ll M^4\) we get
\[
(#(A + B))^8 \geq M^{9+o(1)} \Delta_1^4 \Delta_2^8.
\] (20)

Case 2:
\[
\# \left( \frac{A_1 - A_1}{A_1 - A_1} \right) \geq \text{ord}_p \left( \frac{a''_0/a'_0} {a''_0/a'_0} \right)
\]

Then we have \(M^4 \geq \text{ord}_p \left( \frac{a''_0/a'_0} {a''_0/a'_0} \right)\) and writing \(a''_0 = g^{x''}\) and \(a'_0 = g^{x'}\), we have
\[
\text{ord}_p \left( \frac{a''_0/a'_0} {a''_0/a'_0} \right) = \frac{t}{\gcd(t, x''_0 - x'_0)}
\]

and since \(1 \leq |x''_0 - x'_0| \leq M\) we get \(\text{ord}_p \left( \frac{a''_0/a'_0} {a''_0/a'_0} \right) \gg M/t\). Combining this with the previous inequality gives \(M \geq t^{1/5}\). We may suppose \(\Delta_1 \Delta_2 \geq M^{-1/5}\) since otherwise the bound is trivial, so that (11) and (16) give
\[
\#A_2 \gg M \frac{\Delta_1^2 \Delta_2^2}{\log^2 M} \gg M^{3/5} \gg t^{1/20}.
\] (21)

Since \(A_2 \subseteq \{g^x : L_0 + 1 \leq x \leq L_0 + M\}\), we have
\[
\#A_2 = \sum_{a \in A_2} 1 \leq \sum_{a \in A_2} \sum_{\text{ord}_p (a/a'_0) \leq d_0} 1 \leq \sum_{d_0} \sum_{L_1+1 \leq x \leq L_1+M} 1 \leq \left( \frac{Md_0}{t} + 1 \right) \tau(t)
\]

with \(\tau(t)\) counting the number of divisors of \(t\). By (21) and the bound \(\tau(t) \ll t^{o(1)}\) [4, Theorem 315] we obtain \(1 \ll |A_2|/\tau(t)\) and hence
\[
d_0 \geq \frac{t}{M} \left( \frac{#A_2}{\tau(t)} - 1 \right) \gg \frac{t#A_2}{\tau(t)} M.
\] (22)
By assumption on \(d_0\) and (10) we have
\[
\# \left( \frac{A_1 - A_1}{A_1 - A_1} \right) \gg \frac{t(\#A_1)^2}{\tau(t)M^2}.
\]

Taking \(G = A_1 - A_1 / A_1 - A_1\) in [3 Lemma 3.3] we see that there exists \(\lambda \in (A_1 - A_1)/(A_1 - A_1)\) such that
\[
\# (A + \lambda A) \geq \# (A_1 + \lambda A_1) \geq \min \left\{ \frac{(\#A_1)^2}{\tau(t)M^2}, \frac{t(\#A_1)^2}{\tau(t)M^2} \right\}.
\]

Hence there exist \(a_1, a_2, a_3, a_4 \in A_1\) such that
\[
\# ((a_1 - a_2)A + (a_3 - a_4)A) \gg (\#A_1)^2
\]
or
\[
\# ((a_1 - a_2)A + (a_3 - a_4)A) \gg \frac{t(\#A_1)^2}{\tau(t)M^2}.
\]

For the first case, by (13) and (19)
\[
(\#A_1)^2 \leq \frac{\#(A_0A + a_1A) \#(A_0A - a_2A) \#(A_0A + a_3A) \#(A_0A - a_4A)}{(\#A_1)^3}
\]
\[
\leq \frac{(\#(A + B))^8}{(\#A)^3N^3}
\]
and by (7), (10) and (12) we get
\[
(\#(A + B))^8 \gg M^{9+o(1)} \Delta_1^5 \Delta_2^8 \gg M^{9+o(1)} \Delta_1^5 \Delta_2^8 \tag{23}
\]
similarly for the second case, we get
\[
(\#(A + B))^8 \gg \frac{t}{\tau(t)} M^{7+o(1)} \Delta_1^5 \Delta_2^8
\]
and recalling that \(M \geq t^{1/5}\) and \(\tau(t) \ll t^{o(1)}\), we may absorb the term \(1/\tau(t)\) into \(M^{o(1)}\), which gives
\[
(\#(A + B))^8 \gg tM^{7+o(1)} \Delta_1^5 \Delta_2^8 \tag{24}
\]
and the result follows combining (20), (23) and (24).

Given \(A, B \subset \mathbb{F}_p\), we write
\[
\mathcal{E}_+(A, B) = \# \{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 : a_1 + b_1 = a_2 + b_2\}.
\]
Then we have [11 Lemma 7.1]
Lemma 6. Let \( A, B \subset \mathbb{F}_p \), then
\[
\left| \sum_{a \in A} \sum_{b \in B} e_p(xy) \right|^8 \leq p(\#A)^4(\#B)^4 \mathcal{E}_+(A, A) \mathcal{E}_+(B, B)
\]

Lemma 7. Suppose \( g \in \mathbb{F}_p^* \) has order \( t \) and let \( A \subset \mathbb{F}_p^* \) be the subgroup generated by \( g \). Then for \( N \leq t \) we have
\[
\max_{\gcd(\lambda, p) = 1} |S_{g,p}(\lambda, N)| \ll \begin{cases}
p^{1/8} \mathcal{E}_+(A, A)^{1/4} \log t \\
p^{1/4} t^{-1/4} \mathcal{E}_+(A, A)^{1/4} \log t.
\end{cases}
\]

Proof. Let
\[
\sigma(a, c) = \sum_{n=1}^{t} e_t(an) e_p(cg^n)
\]
then we have
\[
S_{g,p}(\lambda, N) = \sum_{n=1}^{N} e_p(\lambda g^n) = \frac{1}{t} \sum_{k=1}^{t} \sum_{j=1}^{N} e_t(-kj) \sum_{n=0}^{t-1} e_t(kn) e_p(\lambda g^n)
\]
so that
\[
|S_{g,p}(\lambda, N)| \leq \frac{1}{t} \sum_{k=1}^{t} \left| \sum_{j=1}^{N} e_t(-kj) \right| \max_{k \in \mathbb{F}_p} |\sigma(k, \lambda)|
\ll \log t \max_{k \in \mathbb{F}_p} |\sigma(k, \lambda)|.
\] (25)

By [9 Lemma 3.14] for any integers \( k, \lambda \), with \( \gcd(\lambda, p) = 1 \), we have
\[
|\sigma(k, \lambda)| \leq p^{1/4} t^{-1/4} \mathcal{E}_+(A, A)^{1/4},
\]
\[
|\sigma(k, \lambda)| \leq p^{1/8} \mathcal{E}_+(A, A)^{1/4}
\]
and the result follows combining these bounds with (25).

4 Proof of Theorem 1

Let \( J(g, N) \) equal the number of solutions to the equation
\[
g^{x_1} + g^{x_2} = g^{x_3} + g^{x_4}, \quad 1 \leq x_1, x_2, x_3, x_4 \leq N,
\]
then we have
\[ \sum_{\lambda \in \mathbb{F}_p} |S_{\lambda}(p; g, N)|^4 \leq \sum_{\lambda \in \mathbb{F}_p} |S_{\lambda}(p; g, N)|^4 = pJ(g, N). \] (26)

Given \( \mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p \) and \( \mathcal{E}_0 \subset \mathcal{A} \times \mathcal{B} \) we write
\[ \mathcal{A} + \mathcal{E}_0 \mathcal{B} = \{ a + b : (a, b) \in \mathcal{E}_0 \} \]
so that by [1, Lemma 2.4] there exists \( \mathcal{E}_0 \subseteq \mathcal{A} \times \mathcal{A} \) such that
\[ \mathcal{E}_+(\mathcal{A}, \mathcal{A}) \leq \frac{8(\# \mathcal{E}_0)^2}{\#(\mathcal{A} + \mathcal{E}_0 \mathcal{A})} \log^2(e \# \mathcal{A}) \]
and writing \( K = \frac{N^2}{\# \mathcal{E}_0} \) gives
\[ J(g, N) \leq \frac{N^{4+o(1)}}{\#(\mathcal{A} + \mathcal{E}_0 \mathcal{A})} K^2. \] (27)

Since \( N \leq t \) we have \( \# \mathcal{A} = N \) so that \( \# \mathcal{E}_0 = (\# \mathcal{A})^2/K \). Hence by [1, Lemma 2.3] there exists \( \mathcal{A}_1, \mathcal{A}_2 \subseteq \mathcal{A} \) and integer \( Q \) with
\[ \# \mathcal{A}_1 \gg \frac{N}{K}, \quad \# \mathcal{A}_2 \gg \frac{N^2}{QK^2 \log N}, \] (28)
such that
\[ (\# (\mathcal{A} + \mathcal{E}_0 \mathcal{A}))^3 \gg (\# (\mathcal{A}_1 + \mathcal{A}_2)) \frac{QN}{K^3 \log N}. \] (29)

By (28) and Lemma 5 we have
\[ (\# (\mathcal{A}_1 + \mathcal{A}_2))^3 > K \frac{K^3}{24} - 2 \frac{K^{30}}{24} \left( \frac{N^2}{Kt} \right)^{1/24} + 1 \] (30)
and from (29) and (30) we get
\[ (\# (\mathcal{A} + \mathcal{E}_0 \mathcal{A}))^{-1} < K^{36/24} \left( \frac{N^2}{Kt} \right)^{1/24} + 1 \] (31)

Combining (27) with (31) gives
\[ J(g, N) < K^{36/24 - 2} N^{3 - 1/24} \left( \frac{N^2}{Kt} \right)^{1/24} + 1 \leq N^{3 - 1/24} \left( \frac{N^2}{t} \right)^{1/24} + 1 \]
and since \( K \geq 1 \) the result follows.
5 Proof of Theorem 2

We follow the method of [6] and begin with considering

$$\sigma_{p,g}(N) = \max_{1 \leq K \leq N} \max_{\gcd(\lambda, p) = 1} |S_{p,g}(\lambda, K)|$$

so that for any integer $K$ we have

$$\left| S_{p,g}(\lambda, N) - \frac{1}{K} \sum_{k=1}^{K} \sum_{n=1}^{N} e_p(\lambda g^{k+n}) \right| \leq 2\sigma_{g,p}(K).$$

Taking $A = \{g^n : 1 \leq n \leq N\}$, $B = \{\lambda g^n : 1 \leq n \leq K\}$ in Lemma 6 we have by Theorem 1

$$\left| \frac{1}{K} \sum_{k=1}^{K} \sum_{n=1}^{N} e_p(\lambda g^{k+n}) \right| \leq p^{1/8} N^{167/192 + o(1)} \left( 1 + \left( \frac{N^2}{t} \right)^{1/96} \right) K^{-25/192 + o(1)} \left( 1 + \left( \frac{K^2}{t} \right)^{1/192} \right)$$

and letting $K = \lfloor N/3 \rfloor$ we get

$$\sigma_{p,g}(N) \leq \sigma_{p,g}(\lfloor N/3 \rfloor) + p^{1/8} N^{71/96 + o(1)} \left( 1 + \left( \frac{N^2}{t} \right)^{1/96} \right).$$

Repeating the above argument recursively, we end up with $O(\log N)$ terms all bounded by

$$p^{1/8} N^{71/96} \left( 1 + \left( \frac{N^2}{t} \right)^{1/96} \right)$$

which gives

$$\max_{\gcd(\lambda, p) = 1} |S_{g,p}(\lambda, N)| \leq p^{1/8} N^{71/96 + o(1)} \left( 1 + \left( \frac{N^2}{t} \right)^{1/96} \right). \quad (32)$$

Also, we have from Hölder’s inequality,

$$\left| \sum_{k=1}^{K} \sum_{n=1}^{N} e_p(\lambda g^{k+n}) \right| \leq K^3 \sum_{k=1}^{K} \sum_{n=1}^{N} e_p(\lambda g^{k+n}) \leq \sum_{a \in \mathbb{F}_p} |S_{p,g}(a, N)|^4.$$
so by Theorem 1 we get
\[
\left| \sum_{k=1}^{K} \sum_{n=1}^{N} e_p(\lambda g^{k+n}) \right| \leq p^{1/4} K^{-1/4+o(1)} N^{71/96+o(1)} \left( 1 + \left( \frac{N^2}{t^2} \right)^{1/96} \right)
\]
and taking \( K = \lfloor N/3 \rfloor \) gives
\[
\sigma_{p,g}(N) \leq \sigma_{p,g}(\lfloor N/3 \rfloor) + p^{1/4} N^{47/96+o(1)} \left( 1 + \left( \frac{N^2}{t^2} \right)^{1/96} \right).
\]
As before we end up with the bound
\[
\max_{\gcd(\lambda,p)=1} \left| S_{g,p}(\lambda, N) \right| \leq p^{1/4} N^{47/96+o(1)} \left( 1 + \left( \frac{N^2}{t^2} \right)^{1/96} \right) \tag{33}
\]
and the result follows combining (32) and (33).

6 Proof of Theorem 3

Let \( A \subset \mathbb{F}_p^* \) be the subgroup generated by \( g \), so by [8, Theorem 34] we have
\[
\mathcal{E}_+(A, A) \ll \begin{cases} t^{22/9} (\log p)^{2/3}, & \text{if } t \leq p^{3/5} (\log p)^{-6/5}, \\ t^3 p^{-1/3} (\log p)^{4/3}, & \text{if } t > p^{3/5} (\log p)^{-6/5}. \end{cases} \tag{34}
\]
We consider first when \( t \leq p^{1/2} \). Combining Lemma 7 with (34) gives
\[
\max_{\gcd(\lambda,p)=1} \left| S_{g,p}(\lambda, N) \right| \leq p^{1/8} t^{22/36} (\log p)^{7/6}.
\]
For \( p^{1/2} < t \leq p^{3/5} (\log p)^{-6/5} \) we have,
\[
\max_{\gcd(\lambda,p)=1} \left| S_{g,p}(\lambda, N) \right| \leq p^{1/4} t^{13/36} (\log p)^{7/6}.
\]
If \( p^{3/5} (\log p)^{-6/5} < t \leq p^{2/3} (\log p)^{-2/3} \)
\[
\max_{\gcd(\lambda,p)=1} \left| S_{g,p}(\lambda, N) \right| \leq p^{1/6} t^{1/2} (\log p)^{4/3}
\]
and for \( p^{2/3} (\log p)^{-2/3} < t \), from [7, Lemma 2]
\[
\max_{\gcd(\lambda,p)=1} \left| S_{g,p}(\lambda, N) \right| \leq p^{1/2} \log p
\]
and the result follows combining the above bounds.
References

[1] J. Bourgain and M. Z. Garaev, ‘On a variant of sum-product estimates and explicit exponential sum bounds in prime fields’, Math. Proc. Cambr. Phil. Soc., 146 (2008), 1–21.

[2] M. Z. Garaev, ‘An explicit sum-product estimate in $\mathbb{F}_p$’, Intern. Math. Res. Notices, 2007 (2007), Article rnm035, 1–11.

[3] A. Glibichuk and S. V. Konyagin, ‘Additive properties of product sets in fields of prime order’, Additive combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, 279–286.

[4] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford Univ. Press, Oxford, 1979.

[5] D. R. Heath-Brown and S. V. Konyagin, ‘New bounds for Gauss sums derived from $k$th powers, and for Heilbronn’s exponential sum’, Quart. J. Math., 51 (2000), 221–235.

[6] S. V. Konyagin and I. E. Shparlinski, ‘On the consecutive powers of a primitive root: Gaps and exponential sums’, Mathematika, 58 (2012), 11–20.

[7] N. M. Korobov, ‘On the distribution of digits in periodic fractions’, Matem. Sbornik, 89 (1972), 654–670 (in Russian).

[8] I. D. Shkredov, ‘Some new inequalities in additive combinatorics’, arXiv:1208.2344, v3

[9] I. E. Shparlinski, ‘Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness’, Birkhäuser Verlag, 2003

[10] I. E. Shparlinski and W. Steiner, ‘On digit patterns in expansions of rational numbers with prime denominator’, Quart. J. Math., (to appear).

[11] T. Tao and V. Vu, Additive combinatorics, Cambridge Univ. Press, Cambridge, 2006.