On two problems of Mordell about exponential sums

by

Hong Bing Yu (Hefei)

1. Introduction. In his last papers, Mordell ([2, 3]) considered a new type of exponential sums and propounded several interesting problems, two of which we shall discuss in the present note.

Throughout, $p$ is an odd prime, $g$ (and $g_1$) are primitive roots mod $p$, $1 \leq X \leq p - 1$, and $e_r(x) = \exp(2\pi ix/r)$ as usual.

The first problem suggested by Mordell (see [2]) is to estimate

$$(1) \quad S_1 = \sum_{x=1}^{X} e_p(ax + bg^x + cg_1^x), \quad abc \not\equiv 0 \pmod{p},$$

which is an associated exponential sum of

$$(2) \quad S_0 = \sum_{x=1}^{X} e_p(ax + bg^x), \quad ab \not\equiv 0 \pmod{p}.$$

In [2] Mordell proved that

$$|S_0| \leq 2\sqrt{p}\log p + 2\sqrt{p} + 1;$$

he also remarked that the method he used does not appear to be applicable to $S_1$. We shall prove

**Theorem 1.** Let $d = \min(\text{ind}_g g_1, \text{ind}_{g_1} g)$, $d > 1$. Then

$$|S_1| \leq d^{1/4}p^{3/4}(2\log p + 3).$$

The second problem relates to

$$(3) \quad S_n(X, b) = \sum_{x=1}^{X} e_p(bx + f_n(g^x)),$$

where $b \not\equiv 0 \pmod{p}$, and

$$(4) \quad f_n(x) = a_n x^n + \ldots + a_1 x \in \mathbb{Z}[x], \quad a_n \not\equiv 0 \pmod{p}, \quad n < p.$$
Mordell [3] proved, by using an elementary argument, that
\[ |S_n(p - 1, b)| \ll p^{1-1/(2n)} \]
where the implied constant depends only on \( n \). Further he asked whether \( 1/2 \) is the best possible value of the exponent in (5). The following Theorem 2 answers this question affirmatively.

**Theorem 2.** We have
\[ |S_n(X, b)| \leq n\sqrt{p}(2 \log p + 3); \]
and, for \( X > 8n^2 \log^2 p \),
\[ \max_{1 \leq b \leq p-1} |S_n(X, b)| \geq \sqrt{X}/2. \]

Theorem 2 is easily generalized. We have

**Theorem 3.** Let \( f_n(x) \) be as in (4), and let
\[ h_m(x) = b_mx^m + \ldots + b_1x \in \mathbb{Z}[x], \quad b_m \not\equiv 0 \pmod{p}, \quad m < p. \]
Write
\[ S_{m,n}(X) = \sum_{x=1}^{X} e_p(h_m(x) + f_n(g^x)). \]
Then
\[ |S_{m,n}(X)| \leq 4p^{1-1/2^m}(n \log p)^{1/2^{m-1}}. \]

By Theorem 3, (13) (below) and Weyl’s criterion we immediately have the following result, which may be of independent interest.

**Corollary.** For any fixed \( f_n(x) \) satisfying (4) and an arbitrary \( h_m(x) \in \mathbb{Z}[x] \), the numbers \( h_m(x) + f_n(g^x) \) are uniformly distributed modulo \( p \) for \( 1 \leq x \leq p \), when \( p \) is sufficiently large.

It should be mentioned here that, in different contexts, the exponential sums (8) (and hence (1), (2) and (3)) have been generalized by Niederreiter (see Lidl and Niederreiter [1, Chapter 8, \( \S \)7]). However, his results do not imply ours.

**2. The proof of Theorems 1 and 2.** To prove Theorem 1 we need the following lemma.

**Lemma 1.** Let \( \chi \) be a Dirichlet character \((\text{mod } p)\), \( b, c \) and \( d \) be integers with \( bc \not\equiv 0 \pmod{p} \), \( d > 1 \) and \( (p-1,d) = 1 \). Write
\[ S_{\chi}(b,c) = \sum_{x=1}^{p-1} \chi(x)e_p(bx + cx^d). \]
Then
\[ |S_{\chi}(b, c)| \leq d^{1/4} p^{3/4}. \]

Proof. This can be proved by a well-known method due to Mordell. It
is easily seen that
\[
\sum_{u=0}^{p-1} \sum_{v=0}^{p-1} |S_{\chi}(u, v)|^4 \leq p^2 \sum_{s=0}^{p-1} \sum_{t=0}^{p-1} N^2(s, t),
\]
where \(N(s, t)\) denotes the number of solutions of the congruences
\[
\begin{cases}
  x + y \equiv s \pmod{p}, \\
  x^d + y^d \equiv t \pmod{p}.
\end{cases}
\]
Since \(d\) is odd, it follows that \(N(0, 0) = p\), \(N(s, t) = 0\) when only one of \(s, t\)
is zero and \(N(s, t) \leq d - 1\) when \(st \neq 0\). Hence the right hand side of (9) is
\[
\leq p^2 \left( N^2(0, 0) + (d - 1) \sum_{s,t=1}^{p-1} N(s, t) \right)
\]
\[
\leq p^2 (p^2 + (d - 1)(p - 1)(p - 2)) \leq p^4 (p - 1) d.
\]
On the other hand, for any \(k \not\equiv 0 \pmod{p}\), we have \(|S_{\chi}(b, c)| = |S_{\chi}(bk, ck^d)|\).
Also, for given \(u, v\), the congruences
\[
\begin{cases}
  bk \equiv u \pmod{p}, \\
  ck^d \equiv v \pmod{p},
\end{cases}
\]
have at most one solution in \(k\). Hence
\[
|S_{\chi}(b, c)|^4 = \frac{1}{p-1} \sum_{k=1}^{p-1} |S_{\chi}(bk, ck^d)|^4 \leq \frac{1}{p-1} \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} |S_{\chi}(u, v)|^4 \leq p^3 d,
\]
as required.

Proof of Theorem 1. We may assume without loss of generality that \(d = \text{ind}_g g_1\). By the finite Fourier expansion of \(e_p(bg^x + cg^{dx})\), we have, for \(x = 1, \ldots, X\),
\[
e_p(bg^x + cg^{dx}) = \sum_{k=1}^{p-1} c_k e_{p-1}(kx),
\]
where the Fourier coefficients \(c_k\) are given by the formula
\[
c_k = \frac{1}{p-1} \sum_{y=1}^{p-1} e_p(bg^y + cg^{dy}) e_{p-1}(-ky), \quad k = 1, \ldots, p - 1.
\]
By Lemma 1 (setting \(\chi(x) = e_{p-1}(-k \text{ind}_g x)\) and \(d = \text{ind}_g g_1\)) we have
\[
|c_k| \leq \frac{1}{p-1} d^{1/4} p^{3/4} \quad \text{for } k = 1, \ldots, p - 1.
\]
Thus, by (1) and (10) (noting that \(g_1^x \equiv g^{dx} \mod p\)), we get
\[
S_1 = \sum_{x=1}^{X} \sum_{k=1}^{p-1} c_k e_{p-1}(kx) e_p(ax) = \sum_{k=1}^{p-1} c_k \sum_{x=1}^{X} e_{p-1}(kx) e_p(ax).
\]
From this and (11), we have
\[
|S_1| \leq \frac{1}{p-1} d^{1/4} p^{3/4} \sum_{k=1}^{p-2} |\sin \left( \frac{\pi}{p} + \frac{k}{p-1} \right)| + \frac{3}{p-1} d^{1/4} p^{3/4} X,
\]
where the accent indicates that two values of \(k\), to be chosen the same as in Mordell [2, pp. 86–87], are omitted from the summation (cf. [2, (8)]). Then, by the estimate in [2], we have
\[
|S_1| \leq 2d^{1/4} p^{3/4} \log p + 3d^{1/4} p^{3/4} = d^{1/4} p^{3/4} (2 \log p + 3).
\]
This proves Theorem 1.

**Proof of Theorem 2.** We first prove (6), which is in fact a consequence of Weil’s bounds on exponential sums and hybrid sums.

In analogy to (10), we have, for \(x = 1, \ldots, X\),
\[
e_p(f_n(g^x)) = \sum_{k=1}^{p-1} c_k' e_{p-1}(kx),
\]
where the \(c_k'\) are given by
\[
c_k' = \frac{1}{p-1} \sum_{y=1}^{p-1} e_p(f_n(g^y)) e_{p-1}(-ky), \quad k = 1, \ldots, p - 1.
\]
By Weil’s bounds (see Schmidt [4, Corollary II.2F and Theorem II.2G]), we have
\[
|c_k'| \leq \frac{n\sqrt{p}}{p-1}, \quad k = 1, \ldots, p - 1.
\]
Then, similar to the above,
\[
|S_n(X, b)| = \left| \sum_{k=1}^{p-1} c_k' \sum_{x=1}^{X} e_{p-1}(kx) e_p(bx) \right| \leq 2n\sqrt{p} \log p + 3n\sqrt{p}
\]
as required.

To prove (7), we note that
\[
\sum_{b=0}^{p-1} |S_n(X, b)|^2 = \sum_{x,y=1}^{X} \sum_{b=0}^{p-1} e_p(b(x - y) + f_n(g^x) - f_n(g^y)) = pX.
\]
Moreover, from Weil’s bounds mentioned above, it is easily seen that

\[(13) \quad \left| \sum_{x=1}^{X} e_p(f_n(g^x)) \right| \leq 2n\sqrt{p} \log p.\]

This together with (12) gives (7) at once.

3. The proof of Theorem 3. We require the lemma below.

**Lemma 2.** Let \(F(x)\) be an arbitrary function, and let \(\Delta_h F(x) = F(x + h) - F(x)\). Then

\[
\left| \sum_{x=1}^{Y} e(F(x)) \right|^2 = Y + \sum_{r=1}^{Y-1} \sum_{y=1}^{Y-r} e(\Delta_r F(y)) + \sum_{r=1}^{Y-1} \sum_{y=Y+1-r}^{Y} e(\Delta_{r-Y} F(y)),
\]

where \(Y\) is a positive integer and \(e(u) = \exp(2\pi i u)\).

**Proof.** We have

\[(14) \quad \left| \sum_{x=1}^{Y} e(F(x)) \right|^2 = Y + \sum_{x,y=1}^{Y} e(F(x) - F(y)).\]

When \(x \neq y, 1 \leq |x - y| \leq Y - 1\). For any \(r (1 \leq r \leq Y - 1)\), the solutions of \(x - y = r\) are given by \(1 \leq y \leq Y - r\); and the solutions of \(x - y = -Y + r\) are given by \(Y + 1 - r \leq y \leq Y\). The lemma then follows from (14).

To prove Theorem 3, we proceed by induction on \(m\). When \(m = 1\) the result follows from Theorem 2. Assume that Theorem 3 is true with \(m\) replaced by \(m - 1\) (\(m \geq 2\)). By Lemma 2, we have

\[(15) \quad |S_{m,n}(X)|^2 = X + \sum_{r=1}^{X-1} \sum_{y=1}^{X-r} e_p(\Delta_r h_m(y) + \Delta_r f_n(g^y))
+ \sum_{r=1}^{X-1} \sum_{y=X+1-r}^{X} e_p(\Delta_{r-X} h_m(y) + \Delta_{r-X} f_n(g^y)).\]

Write \(T(r)\) for the inner sum of the first double sum in (15). Note that

\(\Delta_r(f_n(g^y)) = a_1(g^r - 1)g^y + \ldots + a_n(g^{nr} - 1)g^{ny}\).

Let \(a_{k_s} (1 \leq s \leq t \leq n)\) be all those \(a_i\) such that \(a_{k_s} \neq 0 \pmod{p}\), and let \(l = (k_1, \ldots, k_t)\). For \(1 \leq r \leq X\), if

\[(16) \quad g^{k_x r} \equiv 1 \pmod{p} \quad \text{for } s = 1, \ldots, t,
\]

then \((p-1) \mid rl\), and so \(\frac{p-1}{(p-1,l)} \mid r\). Thus the number of solutions of (16) is at most \((l, p-1) \leq l \leq n\). For these solutions \(r\), obviously \(|T(r)| \leq X - r \leq X\). For the remaining \(r\)'s, \(a_{k_s}(g^{k_x r} - 1) (1 \leq s \leq t)\) are not all \(\equiv 0 \pmod{p}\).
Moreover, $\Delta_r h_m(y) \pmod{p}$ has degree $m - 1$ with respect to $y$. Hence, by the induction hypothesis,

$$|T(r)| \leq 4p^{1-1/2^m-1}(n \log p)^{1/2^m-2}.$$  

Therefore,

$$\left| \sum_{r=1}^{X-1} T(r) \right| \leq nX + 4p^{1-1/2^m-1}(n \log p)^{1/2^m-2} X.$$  

A similar estimate holds for the second double sum in (15). The result then follows easily.

**Acknowledgements.** The author thanks the referee for the careful reading of the manuscript and useful suggestions.

**References**


[2] L. J. Mordell, *On the exponential sum* $\sum_{x=1}^{X} \exp\left(2\pi i (ax + bg^x)/p\right)$, Mathematika 19 (1972), 84–87.
