ON A PROBLEM OF MORDELL WITH PRIMITIVE ROOTS

CRISTIAN COBELI

ABSTRACT. We consider the sums of the form

\[ S = \sum_{x=1}^{N} \exp \left( (ax + b_1 g_1^x + \cdots + b_r g_r^x) / p \right), \]

where \( p \) is prime and \( g_1, \ldots, g_r \) are primitive roots \( \pmod{p} \). An almost forty years old problem of L. J. Mordell asks to find a nontrivial estimate of \( S \) when at least two of the coefficients \( b_1, \ldots, b_r \) are not divisible by \( p \). Here we obtain a nontrivial bound of the average of these sums when \( g_1 \) runs over all primitive roots \( \pmod{p} \).

1. Introduction

Let \( p \) be a prime number, \( 1 \leq N \leq p - 1 \), \( r \) a positive integer and consider the exponential sum

\[ S_N(a, b, g) := \sum_{x=1}^{N} e_p \left( ax + b g_1^x + \cdots + b g_r^x \right), \quad (1.1) \]

where \( a \), and the components of \( b = (b_1, \ldots, b_r) \) are integers, \( b_1, \ldots, b_r \) are not divisible by \( p \) and \( g = (g_1, \ldots, g_r) \) has components primitive roots modulo \( p \). (We use I. M. Vinogradov's notation \( e_p(\alpha) := \exp(2\pi i \alpha / p) \).) In the case \( r = 1 \), when \( p \nmid a \) and \( p \nmid b \), R. G. Stoneham\([5]\) proved that

\[ S_N(b, g) := \sum_{x=1}^{N} e_p (bg^x) = O(p^{1/2} \log p). \quad (1.2) \]

In a correspondence with D. A. Burgess, L. J. Mordell was informed that both Stoneham and Burgess have found independently several proofs of (1.2). Mordell \([3]\) rediscovered one of the proofs of Burgess and observed that this leads to the following generalization:

\[ S_N(a, b, g) := \sum_{x=1}^{N} e_p (ax + bg^x) < 2p^{1/2} \log p + 2p^{1/2} + 1, \quad (1.3) \]

where \( p \nmid ab \). He remarks that his method doesn’t seem to apply for the estimate of (1.1) when \( r \geq 2 \), and the problem remained unsolved till this day. In this paper, fixing all but one of the primitive roots, say \( g \in \{g_1, \ldots, g_r\} \), we derive a nontrivial bound of \( S = S_N(a, b, g) \) on average over all \( g \) primitive roots \( \pmod{p} \).

Date: December 30, 2009.
In the following we write shortly \( g^x = (g_1^x, \ldots, g_r^x) \), for any integer \( x \) and \( g = (g_1, \ldots, g_r) \). Also, we use the dot product notation: \( b g^x = b_1 g_1^x + \cdots + b_r g_r^x \), where \( b = (b_1, \ldots, b_r) \). Let

\[
S_N(a, b, b, g, g) = \frac{1}{\varphi(p-1)} \sum_{g \pmod{p}}' \sum_{x=1}^{N} e_p(ax + bg^x + b g^x),
\]  

(1.4)

where the prime indicates that the summation is over all \( g \) primitive roots \( (\pmod{p}) \).

**Theorem 1.** Let \( p \) be prime, \( 1 \leq N \leq p-1 \), let \( a, b, b_1, \ldots, b_r \) be integers not all divisible by \( p \), \( \gcd(b, p) = 1 \), and let \( g, g_1, \ldots, g_r \) be primitive roots \( (\pmod{p}) \). Then:

\[
|S_N(a, b, b, g, g)| \ll p^{\frac{23}{24} + \varepsilon}.
\]

(1.5)

The idea of proof is inspired from the Vinogradov’s method and it proved successfully in the estimation of some exponential function analogue of Kloosterman sum, Shparlinski [4].

2. The Complete Interval Case

We may assume that \( r \geq 1 \), since otherwise (1.3) gives a better estimate than (1.5). Taking some fixed primitive root \( g_0 \pmod{p} \), then any primitive root \( g \pmod{p} \) can be written as \( g = g_0^u \pmod{p} \), for some \( 1 \leq u \leq p-1 \) with \( \gcd(u, p - 1) = 1 \). This allows us to replace the sum over \( g \) in (1.4) by a sum over \( 1 \leq u \leq p-1 \) with \( \gcd(u, p - 1) = 1 \). Then

\[
S_N(a, b, b, g, g) = \frac{1}{\varphi(p-1)} \sum_{u=1}^{p-1} \sum_{\gcd(u, p-1) = 1}^{N} e_p(ax + bg^u + b g^u),
\]

(2.1)

\[
\ll \frac{\Sigma_N}{\varphi(p-1)},
\]

where

\[
\Sigma_N = \sum_{u=1}^{p-1} \left| \sum_{\gcd(u, p-1) = 1}^{N} e_p(ax + bg^u + b g^u) \right|.
\]
From now on, in this section we assume that \(N = p - 1\) and write shortly \(\Sigma = \Sigma_{p-1}\). Applying the Cauchy-Schwarz inequality, we have:

\[
\Sigma^2 \leq \varphi(p-1) \sum_{\gcd(u,p-1)=1}^{p-1} \left| \sum_{x=1}^{p-1} e_p(ax + bg^{ux} + bg^{x}) \right|^2
\]

\[
= \varphi(p-1) \sum_{\gcd(u,p-1)=1}^{p-1} \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} e_p(ax + bg^{ux} - ay - bg^{y}) e_p(bg^{ux} - bg^{uy})
\]

\[
\leq \varphi(p-1) \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \left| e_p(a(x - y) + bg^{x} - bg^{y}) \right| \sum_{\gcd(u,p-1)=1}^{p-1} e_p(b(g^{ux} - g^{uy}))
\]

Then, by the Hölder Inequality, we get

\[
\Sigma^8 \leq \varphi(p-1)^4 \left( \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \left| e_p(b(g^{ux} - g^{uy})) \right| \sum_{\gcd(u,p-1)=1}^{p-1} \right)^4
\]

\[
\leq \varphi(p-1)^4 \left( \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} 1 \right)^3 \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \sum_{\gcd(u,p-1)=1}^{p-1} e_p(b(g^{ux} - g^{uy}))
\]

Replacing \(y\) by \(xy\) and then \(g^x\) by \(\lambda\), we have:

\[
\Sigma^8 \leq p^{10} \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \sum_{\gcd(u,p-1)=1}^{p-1} e_p(b(g^{ux} - g^{uy}))
\]

\[
\leq p^{10} \sum_{\lambda=1}^{p-1} \sum_{y=1}^{p-1} \sum_{\gcd(u,p-1)=1}^{p-1} e_p(b(\lambda^{u} - \lambda^{uy}))
\]

(2.2)

The double sum on \(y\) and \(u\) can be estimated following the proof of Theorem 8 from Canetti et al \([2]\). The result is stated in the following lemma:

**Lemma 2.** For any integers \(b\), \(\gcd(a, b, p) = 1\) and \(\lambda\) primitive root \(\mod p\), we have

\[
H_{a,b} = \sum_{y=1}^{p-1} \sum_{x=1}^{p-1} e_p(a\lambda^{x} + b\lambda^{xy}) \leq O(p^{14/3+\epsilon}).
\]

(2.3)

The estimate (2.3) is a generalization and improvement of Theorem 10 from Canetti, Friedlander, Shparlinski \([1]\).
Proof. Using the properties of the Möbius function and then the Hölder inequality, we have:

\[
H_{a,b} = \sum_{y=1}^{p-1} \left| \sum_{d \mid p-1} \mu(d) \sum_{x=1}^{p-1} e_p \left( a \lambda^x + b \lambda^{xy} \right) \right|^4
\]

\[
\leq \sum_{y=1}^{p-1} \left( \sum_{d \mid p-1} 1 \right)^3 \sum_{d \mid p-1} \sum_{x=1}^{p-1} e_p \left( a \lambda^{dx} + b \lambda^{dxy} \right) \left| \sum_{y=1}^{p-1} \sum_{d \mid p-1} \right|^4
\]

\[
\leq \sigma_0^3(p - 1) \sum_{d \mid p-1} \sum_{y=1}^{p-1} \sum_{x=1}^{p-1} e_p \left( a \lambda^{dx} + b \lambda^{dxy} \right) \left| \sum_{y=1}^{p-1} \sum_{d \mid p-1} \right|^4
\]

where \( \sigma_r(n) = \sum_{d \mid n} d^r \) is the sum of powers of the divisors of \( n \). For any \( d \mid p - 1 \) we denote \( t_d := (p - 1)/d \) and \( \lambda_d := \lambda^d \). Notice that the multiplicative order of \( \lambda^d \) is \( t_d \). Then the sum over \( y \) from the last line above becomes:

\[
\sum_{y=1}^{p-1} \sum_{x=1}^{t_d} e_p \left( a \lambda^{dx} + b \lambda^{dxy} \right) \left| \sum_{y=1}^{p-1} \sum_{d \mid p-1} \right|^4 = d \sum_{y=1}^{t_d} \sum_{x=1}^{t_d} e_p \left( a \lambda_d^x + b \lambda_d^{xy} \right) \left| \sum_{y=1}^{p-1} \sum_{d \mid p-1} \right|^4
\]

\[
= d \sum_{y=1}^{t_d} \frac{1}{t_d} \sum_{z=1}^{t_d} \sum_{x=1}^{t_d} e_p \left( a \lambda_d^{x+z} + b \lambda_d^{(x+z)y} \right) \left| \sum_{y=1}^{p-1} \sum_{d \mid p-1} \right|^4
\]

\[
= d \sum_{y=1}^{t_d} \sum_{z=1}^{t_d} \sum_{x=1}^{t_d} e_p \left( a \lambda_d^{z} \lambda_d^x + b \lambda_d^{z} \lambda_d^{xy} \right) \left| \sum_{y=1}^{p-1} \sum_{d \mid p-1} \right|^4
\]

\[
\leq d \sum_{y=1}^{t_d} \sum_{z=1}^{t_d} \sum_{x=1}^{p-1} e_p \left( a \lambda_d^{x} + b \lambda_d^{xy} \right) \left| \sum_{y=1}^{p-1} \sum_{d \mid p-1} \right|^4
\]

since for each fixed \( y \in \{1, \ldots, t_d\} \) the pairs \( (at_d^z, b\lambda_d^{zy}) \) with \( z \in \{1, \ldots, t_d\} \) are distinct modulo \( p \). Next we write explicitly the absolute value in the last term and see that (2.5)
gives
\[
\sum_{y=1}^{p-1} \left| \sum_{x=1}^{t_d} e_p\left( a \lambda^d x + b \lambda^d xy \right) \right|^4
\leq \frac{d}{t_d} \sum_{\alpha,\beta=0}^{p-1} \sum_{y,x_1,x_2,x_3,x_4=1}^{t_d} e_p\left( \alpha(\lambda_d^{x_1} + \lambda_d^{x_2} - \lambda_d^{x_3} - \lambda_d^{x_4}) + \beta(\lambda_d^{x_1 y} + \lambda_d^{x_2 y} - \lambda_d^{x_3 y} - \lambda_d^{x_4 y}) \right)
\leq \frac{d}{t_d} \cdot p^2 \cdot T_d,
\]
where \( T_d \) is the number of solutions of the system of congruences:
\[
\begin{align*}
\lambda_d^{x_1} + \lambda_d^{x_2} & \equiv \lambda_d^{x_3} + \lambda_d^{x_4}, \\
\lambda_d^{x_1 y} + \lambda_d^{x_2 y} & \equiv \lambda_d^{x_3 y} + \lambda_d^{x_4 y}
\end{align*}
\]
with \( 1 \leq x_1, x_2, x_3, x_4, y \leq t_d \). In the proof of Theorem 8 from Canetti et all \[2\], the last inequality bounds \( T_d \) by
\[
T_d \ll t_d^{14/3} p^{-1}.
\]
Then, by (2.4), (2.6) and (2.7), we obtain
\[
H_{a,b} \ll \sigma_0^3 (p-1) \sum_{d|p-1} \frac{d}{t_d} \cdot p^2 \cdot t_d^{14/3} p^{-1} \ll \sigma_0^3 (p-1) \sigma_{14} (p-1) \cdot p^{14/3}
\]
and the lemma follows, since \( \sigma_r(n) \ll n^r \) for any \( r \).

By (2.4) and (2.6) we deduce that:
\[
\sum^8 \ll p^{10} \sum_{\lambda=1}^{p-1} p^{14/3+\epsilon} \ll p^{47/3+\epsilon}.
\]
Then making use of the estimate \( p/ \log \log p \ll \varphi(p-1) \), we obtain
\[
\frac{\sum}{\varphi(p-1)} \ll p^{23/24+\epsilon}.
\]
From this estimate together with (2.1), it follows (1.5), so Theorem \[1\] is proved in the case \( N = p - 1 \).
3. COMPLETION OF THE PROOF

It remains to show that the size of the incomplete sums is not far from that of the complete ones. Let $I$ be an interval of integers $\subseteq [1, p - 1]$ and denote

$$S(I) = \sum_{u=1}^{p-1} \sum_{x \in I} e_p(ax + bg^{ux} + bg^{x}). \quad (3.1)$$

In order to estimate the departure of $S(I)$ from $S([1, p - 1])$, the following characteristic function of the interval $I$ is suitable:

$$\frac{1}{p} \sum_{y \in I} \sum_{k=1}^{p} e_p(k(y - x)) = \begin{cases} 1, & \text{if } x \in I; \\ 0, & \text{else}. \end{cases}$$

Then

$$S(I) = \sum_{u=1}^{p-1} \sum_{x \in I} e_p(ax + bg^{ux} + bg^{x})$$

$$= \sum_{u=1}^{p-1} \sum_{x=1}^{p-1} e_p(ax + bg^{ux} + bg^{x}) \frac{1}{p} \sum_{y \in I} \sum_{k=1}^{p} e_p(k(y - x))$$

$$= \frac{1}{p} \sum_{k=1}^{p} \sum_{y \in I} e_p(ky) \sum_{u=1}^{p-1} \sum_{x=1}^{p-1} e_p((a - k)x + bg^{ux} + bg^{x}).$$

In this last form of $S(I)$ we separate the terms with $k = p$ and bound its absolute value to get:

$$|S(I)| \leq \frac{1}{p} \sum_{k=1}^{p-1} \left| \sum_{y \in I} e_p(ky) \right| \left| \sum_{u=1}^{p-1} \sum_{x=1}^{p-1} e_p((a - k)x + bg^{ux} + bg^{x}) \right|$$

$$+ \frac{1}{p} |I| \sum_{u=1}^{p-1} \left| \sum_{x=1}^{p-1} e_p(ax + bg^{ux} + bg^{x}) \right|. \quad (3.2)$$

Here the sum over $y$ is a geometric progression, that can be evaluated accurately using

$$|e_p(k) - 1| = 2 \left| \sin \left( \frac{k\pi}{p} \right) \right| \geq 4 \left| \frac{k}{p} \right|. \quad (3.3)$$
where \( \| \cdot \| \) is the distance to the nearest integer, while the sums over \( u \) and \( x \) are the complete sums bounded by (2.8). Thus, by (3.2), (3.3) and (2.8), we get

\[
|S(I)| \leq \frac{1}{p} \sum_{k=1}^{p-1} \left| e_p(k) - 1 \right| p^{47/24+\epsilon} + \frac{1}{p} |I| p^{47/24+\epsilon}
\]

\[
\leq p^{47/24+\epsilon} \left( \frac{1}{p} \sum_{k=1}^{p-1} \frac{1}{2k/p} + 1 \right)
\]

\[
\leq p^{47/24+\epsilon} (3 + \log p)
\]

\[
\leq p^{47/24+\epsilon},
\]

which concludes the proof of Theorem 1.

Acknowledgement: We thank Ke Gong for his careful reading of an earlier version of this paper.

References

[1] R. Canetti, J. B. Friedlander, and I. E. Shparlinski, On certain Exponential Sums and the Distribution of Diffie-Hellman Triples, J. London Math. Soc., 59 (1999), 799–812.

[2] R. Canetti, J. B. Friedlander, S. Konyagin, M. Larsen, D. Lieman and I. E. Shparlinski, On the Statistical Properties of Diffie-Hellman Distributions, Israel J. Math., 120 (2000), 23–46.

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

[4] I. Shparlinski, Exponential Function Analogue of Kloosterman Sums, Rocky Mountain J. Math., 2004, v. 34, 1497–1502.

[5] R. G. Stoneham, On the Uniform \( \epsilon \)-Distribution of Residues within the Periods of Rational Fractions with Applications to Normal Numbers, Acta Arithmetica, 22 (1972), 371–389.

Cristian Cobeli, Mathematics Research Institute of the Romanian Academy, P.O. Box 1-764, Bucharest, 70700, Romania

E-mail address: cristian.cobeli@imar.ro