Goran Djanković

Power-moments of $\mathrm{SL}_3(\mathbb{Z})$ Kloosterman sums

Czechoslovak Mathematical Journal, Vol. 63 (2013), No. 3, 833–845

Persistent URL: `http://dml.cz/dmlcz/143493`

Czechoslovak Mathematical Journal, 63 (138) (2013), 833–845

POWER-MOMENTS OF $SL_3(\mathbb{Z})$ KLOOSTERMAN SUMS

Goran Djanković, Beograd

(Received June 13, 2012)

Abstract. Classical Kloosterman sums have a prominent role in the study of automorphic forms on GL_2 and further they have numerous applications in analytic number theory. In recent years, various problems in analytic theory of automorphic forms on GL_3 have been considered, in which analogous GL_3-Kloosterman sums (related to the corresponding Bruhat decomposition) appear. In this note we investigate the first four power-moments of the Kloosterman sums associated with the group $SL_3(\mathbb{Z})$. We give formulas for the first three moments and a nontrivial bound for the fourth.

Keywords: power-moment; $SL_3(\mathbb{Z})$-Kloosterman sum

MSC 2010: 11L05, 11T23

1. Introduction

The classical Kloosterman sum is defined for integers a, b and a positive integer c by

$$S(a,b;c)=\sum_{x \pmod c}^{*} e\Big(\frac{ax+b\bar{x}}{c}\Big), \tag{1.1}$$

where $\sum^*$ means that the summation is restricted to the residue classes x with $(x,c)=1$, $x\bar{x}\equiv 1 \pmod c$ and $e(z)=\mathrm{e}^{2\pi \mathrm{i} z}$.

These sums first appeared in Kloosterman's paper [5], in his application of the circle method to representations of integers by quadratic forms in four variables. More importantly, they are related to Fourier coefficients of automorphic forms on GL_2 ([4], chapter 3).

This work was partially supported by Ministry of Science, Republic of Serbia, Project no. 174008.

One of the first results about classical Kloosterman sums was the evaluation of the first few power-moments

$$V_k(p) = \sum_{a \ (\mathrm{mod}\ p)}^{*} S(a,1;p)^k, \tag{1.2}$$

for Kloosterman sums to prime modulus p. The case of prime modulus is the key for understanding of these sums because of the twisted multiplicativity formula

$$S(a,b;qr) = S(\bar{q}a,\bar{q}b;r)S(\bar{r}a,\bar{r}b;q), \quad \text{valid for } (q,r)=1,$$

where $\bar{q}q \equiv 1 \pmod r$, $\bar{r}r \equiv 1 \pmod q$ and the following exact evaluation in the case when the modulus is a prime power p^β, $\beta \geqslant 2$:

$$S(a,a;p^\beta) = 2\Big(\frac{a}{p^\beta}\Big)p^{\beta/2}\Re\varepsilon_{p^\beta} e\Big(\frac{2a}{p^\beta}\Big),$$

where $(p,2a)=1$, $(\cdot/p^\beta)$ is the Legendre-Jacobi symbol and $\varepsilon_c = 1$ or i, according to whether $c \equiv 1$ or $-1 \pmod 4$.

We have (e.g. see Chapter 4 in [4])

$$V_1(p) = 1, \tag{1.3}$$

$$V_2(p) = p^2 - p - 1, \tag{1.4}$$

$$V_3(p) = \Big(\frac{-3}{p}\Big)p^2 + 2p + 1, \tag{1.5}$$

$$V_4(p) = 2p^3 - 3p^2 - 3p - 1. \tag{1.6}$$

In particular, by dropping all but one term in the last equality, one obtains

$$|S(a,b;p)| < 2p^{3/4} \quad \text{for } (ab,p)=1.$$

This bound was a crucial ingredient in [5].

1.1. $\mathrm{SL}_3(\mathbb{Z})$ **Kloosterman sums.** Conceptually, the classical $\mathrm{SL}_2(\mathbb{Z})$-Kloosterman sums (1.1) are related to the Bruhat decomposition for $\mathrm{GL}_2(\mathbb{R})$, as explained for example in [3], page 340.

The Weyl group W_3 for $\mathrm{GL}_3(\mathbb{R})$ consists of the following six elements:

$$w_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad w_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad w_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$w_4 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad w_5 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad w_6 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

and then the Bruhat decomposition is given by

$$\mathrm{GL}_3(\mathbb{R}) = \bigsqcup_{w_i \in W_3} G_{w_i}, \quad \text{with} \quad G_{w_i} = U_3 w_i \Delta U_3,$$

where

$$U_3 = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} < \mathrm{GL}_3(\mathbb{R}), \quad \Delta = \left\{ \begin{pmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix} \right\} < \mathrm{GL}_3(\mathbb{R})$$

are the minimal parabolic and diagonal subgroups of $\mathrm{GL}_3(\mathbb{R})$.

Let $\Gamma = \mathrm{SL}_3(\mathbb{Z})$ and $\Gamma_\infty = \Gamma \cap U_3$. For any $w \in W_3$, let $\Gamma_w = (w^{-1} \cdot \Gamma_\infty^t \cdot w) \cap \Gamma_\infty$. For two non-zero integers D_1, D_2 we denote

$$d = \begin{pmatrix} 1/D_2 & 0 & \\ & D_2/D_1 & 0 \\ 0 & 0 & D_1 \end{pmatrix} \in \Delta.$$

Then, for any two characters ψ_1 and ψ_2 of the group U_3, the $\mathrm{SL}_3(\mathbb{Z})$-Kloosterman sum associated with d and a Weyl group element w is defined by

$$S_w(\psi_1, \psi_2; d) = \sum_{\substack{\gamma \in \Gamma_\infty \backslash \Gamma \cap G_w / \Gamma_w \\ \gamma = b_1 w d b_2}} \psi_1(b_1)\psi_2(b_2),$$

provided it is independent of the choice of Bruhat decomposition for matrices γ and otherwise it is set to be zero.

These exponential sums are extremely important in the spectral theory of automorphic forms for $\mathrm{SL}_3(\mathbb{Z})$ since all the six types of Kloosterman sums $S_{w_i}(\psi_1, \psi_2; d)$, $i = 1, \ldots, 6$ appear in the expressions for Fourier-Whittaker coefficients of $\mathrm{SL}_3(\mathbb{Z})$-Poincaré series and consequently, they all appear in the trace formula of Kuznetsov type for the group $\mathrm{SL}_3(\mathbb{Z})$ (cf. [3], Chapter 11).

For a pair $(m_1, m_2) \in \mathbb{Z}^2$, we denote by $\psi_{(m_1,m_2)}$ the following character on U_3:

$$\psi_{(m_1,m_2)}\colon \begin{pmatrix} 1 & u_2 & u_3 \\ 0 & 1 & u_1 \\ 0 & 0 & 0 \end{pmatrix} \mapsto e(m_1 u_1 + m_2 u_2),$$

and in this notation we can write $S_w(m_1, m_2, n_1, n_2; d)$ for $S_w(\psi_{(m_1,m_2)}, \psi_{(n_1,n_2)}; d)$.

It is shown in [2] that the sums $S_{w_i}(m_1, m_2, n_1, n_2; d)$ for $i = 1, 2, 3$ are “degenerate” (i.e. trivial or coincide with the $\mathrm{SL}_2(\mathbb{Z})$-Kloosterman sums), while S_{w_6} and S_{w_4}, S_{w_5} are new exponential sums.

The sums $S_{w_6}(m_1, m_2, n_1, n_2; d)$, corresponding to the so called long element w_6, can be given explicitly as follows (see [2] or [3]): for $m_1, m_2, n_1, n_2 \in \mathbb{Z}$ and $D_1, D_2 \in \mathbb{N}$,

$$\begin{aligned} S(m_1, m_2, n_1, n_2; D_1, D_2) &= \sum\sum\sum\sum_{\substack{B_1, C_1 \ (\mathrm{mod}\ D_1) \\ B_2, C_2 \ (\mathrm{mod}\ D_2) \\ (B_1, C_1, D_1) = (B_2, C_2, D_2) = 1 \\ D_1 C_2 + B_1 B_2 + C_1 D_2 \equiv 0 \ (\mathrm{mod}\ D_1 D_2)}} e\Big(\frac{m_1 B_1 + n_1(Y_1 D_2 - Z_1 B_2)}{D_1}\Big) \\ &\qquad \times e\Big(\frac{m_2 B_2 + n_2(Y_2 D_1 - Z_2 B_1)}{D_2}\Big), \end{aligned}$$

where Y_1, Z_1, Y_2, Z_2 are chosen so that

$$Y_1 B_1 + Z_1 C_1 \equiv 1 \pmod{D_1}, \quad Y_2 B_2 + Z_2 C_2 \equiv 1 \pmod{D_2}.$$

Some of their properties are proved in [2], Section 4. For example, if $p_1 p_2 \equiv q_1 q_2 \equiv 1 \pmod{D_1 D_2}$ then we have

$$S(m_1 p_1, p_2 m_2, n_1 q_1, q_2 n_2; D_1, D_2) = S(m_1, m_2, n_1, n_2; D_1, D_2). \tag{1.7}$$

Also we have

$$\begin{aligned} &S(m_1, m_2, n_1, n_2; D_1 D_1', D_2 D_2') \\ &\quad = S(\overline{D_1'}^2 D_2' m_1, \overline{D_2'}^2 D_1' m_2, n_1, n_2; D_1, D_2) S(\overline{D_1}^2 D_2 m_1, \overline{D_2}^2 D_1 m_2, n_1, n_2; D_1', D_2'), \end{aligned}$$

where

$$(D_1 D_2, D_1' D_2') = 1,$$

and $\overline{D_i}, \overline{D_i'},\ i = 1, 2$ are given by

$$\overline{D_1} D_1 \equiv \overline{D_2} D_2 \equiv 1 \pmod{D_1' D_2'}, \quad \overline{D_1'} D_1' \equiv \overline{D_2'} D_2' \equiv 1 \pmod{D_1 D_2}.$$

In particular, for $(D_1, D_2) = 1$ we have

$$S(m_1, m_2, n_1, n_2; D_1, D_2) = S(D_2 m_1, n_1; D_1) S(D_1 m_2, n_2; D_2). \tag{1.8}$$

The $\mathrm{SL}_3(\mathbb{Z})$-Kloosterman sums corresponding to elements w_4 and w_5 are both of the following form (see [2]):

$$\widetilde{S}(m_1, n_1, n_2; D_1, D_2) = \sum_{\substack{C_1 \ (\mathrm{mod}\ D_1) \\ (C_1, D_1) = 1}} \sum_{\substack{C_2 \ (\mathrm{mod}\ D_2) \\ (C_2, D_2/D_1) = 1}} e\Big(\frac{m_1 C_1 + n_1 \overline{C_1} C_2}{D_1}\Big) e\Big(\frac{n_2 \overline{C_2}}{D_2/D_1}\Big),$$

where $m_1, n_1, n_2 \in \mathbb{Z}$, and $D_1, D_2 \in \mathbb{N}$ such that $D_1 \mid D_2$.

For $p_1q_1 \equiv 1 \pmod{D_1}$ and $p_2q_2 \equiv 1 \pmod{D_2}$ we have

$$\widetilde{S}(m_1p_1, q_1n_1p_2, q_2n_2; D_1, D_2) = \widetilde{S}(m_1, n_1, n_2; D_1, D_2). \tag{1.9}$$

Also for $(D_2, D_2') = 1$ we have

$$\begin{aligned}\widetilde{S}&(m_1, n_1, n_2; D_1D_1', D_2D_2') \\ &= \widetilde{S}(\overline{D_1'}m_1, D_2'n_1, \overline{D_2'}^2 n_2; D_1, D_2)\widetilde{S}(\overline{D_1}m_1, D_2n_1, \overline{D_2}^2 n_2; D_1', D_2').\end{aligned} \tag{1.10}$$

For $p^l \nmid n_1$ we have $\widetilde{S}(m_1, n_1, n_2; p^l, p^l) = 0$. Further, for $1 \leqslant l < k$ we have also

$$\widetilde{S}(m_1, n_1, n_2; p^l, p^k) = 0, \tag{1.11}$$

unless (i) $k < 2l$ and $p^{2l-k}|n_1$, (ii) $k = 2l$ or (iii) $k > 2l$ and $p^{k-2l} \mid n_2$.

1.2. Main results. For $m_1, n_2 \in \mathbb{Z}$ with $(m_1n_2, D_1D_2) = 1$, from (1.7), we see that

$$S(m_1, m_2, n_1, n_2; D_1, D_2) = S(1, m_1m_2, n_1n_2, 1; D_1, D_2),$$

so it is natural to consider the following analogue of (1.2) for a positive integer k and two different prime numbers p and q:

$$U_k(p, q) = \sideset{}{^*}\sum_{a \pmod p} \sideset{}{^*}\sum_{b \pmod p} S(1, a, b, 1; p, q)^k.$$

But using (1.8) we get immediately

$$U_k(p, q) = \sideset{}{^*}\sum_{a \pmod p} \sideset{}{^*}\sum_{b \pmod p} S(q, b; p)^k S(pa, 1, q)^k = V_k(p)V_k(q).$$

Hence, there is nothing new and the formula for $U_k(p, q)$ for $k = 1, 2, 3, 4$ follows from (1.3)–(1.6).

The case of equal prime moduli is also trivial, since there is an explicit formula for such sums, see Property 4.10 in [2]. For example, if $(p, m_1m_2n_1n_2) = 1$, then

$$S(m_1, m_2, n_1, n_2; p, p) = p + 1.$$

Similarly, because of the twisted multiplicativity (1.10) the exponential sums $\widetilde{S}(m_1, n_1, n_2; D_1, D_2)$ corresponding to Weyl group elements w_4 and w_5 reduce to those with moduli of the form $(D_1, D_2) = (p^l, p^k)$ for prime numbers p. Then from (1.11) we see that we do not have an explicit evaluation of the sums

$\widetilde{S}(m_1, n_1, n_2; p, p^2)$ and hence it is interesting to study them on average by calculating their moments.

Explicitly, these Kloosterman sums are given by

$$\widetilde{S}(m_1, n_1, n_2; p, p^2) = p \sum_{x \pmod p}^{*} \sum_{y \pmod p}^{*} e\Big(\frac{m_1 x + n_1 \bar{x} y + n_2 \bar{y}}{p}\Big). \tag{1.12}$$

For $(m_1 n_1 n_2, p) = 1$, from (1.9) we have

$$\widetilde{S}(m_1, n_1, n_2; p, p^2) = \widetilde{S}(m_1 n_1 n_2, 1, 1; p, p^2) \tag{1.13}$$

so it is natural to consider the power-moments

$$W_k(p) := \sum_{a \pmod p}^{*} \widetilde{S}(a, 1, 1; p, p^2)^k,$$

which are analogous to the moments of classical Kloosterman sums (1.2).

In [6], Larsen showed, using a theorem of Deligne, that the following bound holds for all a, $p \nmid a$:

$$|\widetilde{S}(a, 1, 1; p, p^2)| \leqslant 3p^2. \tag{1.14}$$

Also, it should be noted that the sums $\widetilde{S}(a, 1, 1; p, p^2)$ are not real in general, in contrast to the case of classical Kloosterman sums (1.1).

We compute the first three power-moments of the sums $\widetilde{S}(a, 1, 1; p, p^2)$ in the following theorems:

Theorem 1.1. *For a prime number $p > 2$ we have*

$$W_1(p) = -p \quad \textit{and} \quad W_2(p) = -p^4 - p^3 - p^2, \tag{1.15}$$

while

$$\sum_{a \pmod p}^{*} |\widetilde{S}(a, 1, 1; p, p^2)|^2 = p^5 - p^4 - p^3 - p^2. \tag{1.16}$$

Theorem 1.2. *For a prime number $p > 2$ we have*

$$W_3(p) = p^7 - p^6 - \Big(\frac{-3}{p}\Big)p^6 - 3p^5 - 2p^4 - p^3.$$

The exact evaluation of the fourth power-moment $W_4(p)$ reduces to counting the number of points on the variety in $(\mathbb{F}_p^{\times})^8$ given by the equations

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &\equiv 0 \pmod p, \\ y_1 + y_2 + y_3 + y_4 &\equiv 0 \pmod p, \\ \overline{x_1y_1} + \overline{x_2y_2} + \overline{x_3y_3} + \overline{x_4y_4} &\equiv 0 \pmod p. \end{aligned}$$

The number of points on this variety can be expressed as a sum of Jacobsthal sums over $\mathbb{F}_p$, associated with certain polynomials of degree 4, but we are not aware of any explicit evaluations of such sums, so this remains as an open problem.

On the other hand, it follows trivially from Larsen's bound (1.14) that

$$W_4(p) \ll p^9.$$

It is interesting to note that by Theorem 1.2, the analogous trivial bound for $W_3(p)$ is of the true order of magnitude, i.e. curiously there is no cancelation in the sum $\sum_{a(p)}^{*}\widetilde{S}(a,1,1;p,p^2)^3$.

Therefore, it is natural at least to ask if there is some cancelation in the fourth moment $W_4(p)$. An answer in this direction can be given using the work of A. Adolphson and S. Sperber from [1]:

Theorem 1.3. *For a prime number p, we have*

$$W_4(p) \ll p^{17/2}. \tag{1.17}$$

2. Proof of Theorem 1.1

For the first moment, since $\widetilde{S}(0,1,1;p,p^2) = p$, we have trivially, after completion to all residues modulo p,

$$\begin{aligned} W_1(p) &= \sum_{a \pmod p}^{*} \widetilde{S}(a,1,1;p,p^2) = \sum_{a \pmod p} \widetilde{S}(a,1,1;p,p^2) - \widetilde{S}(0,1,1;p,p^2) \\ &= p \sum_{x \pmod p}^{*} \sum_{y \pmod p}^{*} e\Big(\frac{\bar{x}y + \bar{y}}{p}\Big) \sum_{a \pmod p} e\Big(\frac{ax}{p}\Big) - p = -p. \end{aligned}$$

For the second moment we calculate similarly

$$
\begin{aligned}
W_2(p) &= \sum_{a \pmod p} \widetilde{S}(a,1,1;p,p^2)^2 - p^2 \\
&= -p^2 + p^2 \sideset{}{^*}\sum_{\substack{x_1,x_2 \pmod p\\ y_1,y_2 \pmod p}} e\Big(\frac{\overline{x_1}y_1 + \overline{x_2}y_2 + \overline{y_1} + \overline{y_2}}{p}\Big) \sum_{a \pmod p} e\Big(\frac{a(x_1+x_2)}{p}\Big) \\
&= -p^2 + p^3 \sideset{}{^*}\sum_{y_1,y_2 \pmod p} e\Big(\frac{\overline{y_1} + \overline{y_2}}{p}\Big) \sideset{}{^*}\sum_{x \pmod p} e\Big(\frac{x(y_1-y_2)}{p}\Big) \\
&= -p^2 - p^3 \sideset{}{^*}\sum_{y_1,y_2 \pmod p} e\Big(\frac{\overline{y_1} + \overline{y_2}}{p}\Big) + p^4 \sideset{}{^*}\sum_{y \pmod p} e\Big(\frac{2\overline{y}}{p}\Big) \\
&= -p^4 - p^3 - p^2.
\end{aligned}
$$

In the same manner one can get $\sideset{}{^*}\sum_{a \pmod p} |\widetilde{S}(a,1,1;p,p^2)|^2 = p^5 - p^4 - p^3 - p^2.$ □

3. The third power-moment $W_3(p)$ and proof of Theorem 1.2

We start by completing the sum:

$$\sum_{a \pmod p} \widetilde{S}(a,1,1;p,p^2)^3 = W_3(p) + \widetilde{S}(0,1,1;p,p^2)^3 = W_3(p) + p^3.$$

Hence we have

$$
\begin{aligned}
W_3(p) + p^3 &= p^3 \sum_{a \pmod p} \Big[\sideset{}{^*}\sum_{x \pmod p} \sideset{}{^*}\sum_{y \pmod p} e\Big(\frac{ax + \bar{x}y + \bar{y}}{p}\Big)\Big]^3 \\
&= p^3 \sideset{}{^*}\sum_{x_1,x_2,x_3 \pmod p} \sideset{}{^*}\sum_{y_1,y_2,y_3 \pmod p} e\Big(\frac{\overline{x_1}y_1 + \overline{x_2}y_2 + \overline{x_3}y_3 + \overline{y_1} + \overline{y_2} + \overline{y_3}}{p}\Big) \\
&\quad \times \sum_{a \pmod p} e\Big(\frac{a(x_1+x_2+x_3)}{p}\Big) \\
&= p^4 \sideset{}{^*}\sum_{\substack{x_1,x_2,x_3 \pmod p\\ x_1+x_2+x_3 \equiv 0 (p)}} \sideset{}{^*}\sum_{y_1,y_2,y_3 \pmod p} e\Big(\frac{\overline{x_1}y_1 + \overline{x_2}y_2 + \overline{x_3}y_3 + \overline{y_1} + \overline{y_2} + \overline{y_3}}{p}\Big).
\end{aligned}
$$

Here we change the variables by writing

$$x_1 \equiv x,\ x_2 \equiv xz \quad \text{and} \quad x_3 \equiv -x(1+z),$$

with the conditions $x \neq 0$ and $z \neq 0, -1$. We get further that $W_3(p) + p^3$ is equal to

$$
\begin{aligned}
&p^4 \sideset{}{^*}\sum_{x \ (\mathrm{mod}\ p)} \sum_{\substack{z \ (\mathrm{mod}\ p) \\ z \neq 0, -1}} \sideset{}{^*}\sum_{y_1, y_2, y_3 \ (\mathrm{mod}\ p)} e\Big(\frac{\overline{x} y_1 + \overline{x}\,\overline{z} y_2 - \overline{x}\,\overline{1+z}\, y_3 + \overline{y_1} + \overline{y_2} + \overline{y_3}}{p}\Big) \\
&= p^4 \sum_{\substack{z \ (\mathrm{mod}\ p) \\ z \neq 0, -1}} \sideset{}{^*}\sum_{y_1, y_2, y_3 \ (\mathrm{mod}\ p)} e\Big(\frac{\overline{y_1} + \overline{y_2} + \overline{y_3}}{p}\Big) \sideset{}{^*}\sum_{x \ (\mathrm{mod}\ p)} e\Big(\frac{x(y_1 + \overline{z} y_2 - \overline{1+z}\, y_3)}{p}\Big) \\
&= p^5 \sum_{\substack{z \ (\mathrm{mod}\ p) \\ z \neq 0, -1}} \sideset{}{^*}\sum_{\substack{y_1, y_2, y_3 \ (\mathrm{mod}\ p) \\ y_1 + \overline{z} y_2 - \overline{1+z}\, y_3 \equiv 0 \ (\mathrm{mod}\ p)}} e\Big(\frac{\overline{y_1} + \overline{y_2} + \overline{y_3}}{p}\Big) \\
&\quad - p^4 \sum_{\substack{z \ (\mathrm{mod}\ p) \\ z \neq 0, -1}} \sideset{}{^*}\sum_{y_1, y_2, y_3 \ (\mathrm{mod}\ p)} e\Big(\frac{\overline{y_1} + \overline{y_2} + \overline{y_3}}{p}\Big).
\end{aligned}
$$

The contribution of the second line is $p^4(p-2)$, while in the first double sum we introduce the change of variables

$$
y_1 = y, \quad y_2 = yu, \quad y_3 = yv,
$$

where $y, u, v \neq 0 \pmod p$ and $1 + \overline{z}u - \overline{1+z}v \equiv 0 \pmod p$. Therefore, the inner summation becomes

$$
\begin{aligned}
\sideset{}{^*}\sum_{\substack{y_1, y_2, y_3 \ (\mathrm{mod}\ p) \\ y_1 + \overline{z} y_2 - \overline{1+z}\, y_3 \equiv 0 \ (\mathrm{mod}\ p)}} e\Big(\frac{\overline{y_1} + \overline{y_2} + \overline{y_3}}{p}\Big) &= \sideset{}{^*}\sum_{\substack{y, u, v \ (\mathrm{mod}\ p) \\ 1 + \overline{z} u - \overline{1+z} v \equiv 0 \ (\mathrm{mod}\ p)}} e\Big(\frac{\overline{y}(1 + \bar{u} + \overline{v})}{p}\Big) \\
&= p \sideset{}{^*}\sum_{\substack{u, v \ (\mathrm{mod}\ p) \\ 1 + \overline{z} u - \overline{1+z} v \equiv 0 \ (\mathrm{mod}\ p) \\ 1 + \bar{u} + \overline{v} \equiv 0 \ (\mathrm{mod}\ p)}} 1 - \sideset{}{^*}\sum_{\substack{u, v \ (\mathrm{mod}\ p) \\ 1 + \overline{z} u - \overline{1+z} v \equiv 0 \ (\mathrm{mod}\ p)}} 1.
\end{aligned}
$$

In the last summation v is uniquely determined by a pair z, u, with the only constraint being $u \neq -z \pmod p$, since $v \neq 0 \pmod p$. Therefore, for every admissible z, the last sum is $p - 2$ and we obtain

$$
W_3(p) = -p^3 + p^4(p-2) - p^5(p-2)^2 + p^6 \sum_{\substack{z \ (\mathrm{mod}\ p) \\ z \neq 0, -1}} \sideset{}{^*}\sum_{\substack{u, v \ (\mathrm{mod}\ p) \\ 1 + \overline{z} u - \overline{1+z} v \equiv 0 \ (\mathrm{mod}\ p) \\ 1 + \bar{u} + \overline{v} \equiv 0 \ (\mathrm{mod}\ p)}} 1. \tag{3.1}
$$

The conditions in the last summation are equivalent to

$$
u + v + uv \equiv 0 \pmod p
$$

and

$$\begin{aligned}0 &\equiv z^2+(1+u-v)z+u\\ &\equiv z^2+(1+u-v)z-v(u+1)\equiv (z-v)(z+u+1) \pmod p.\end{aligned}$$

If here $v=z$, we must have $u=-z\overline{1+z}$, giving $p-2$ solutions. If $z=-u-1$, we must have $u\not\equiv 0,-1 \pmod p$ and then $v=-\overline{z}(1+z)$, giving another $p-2$ solutions. These two sets of solutions intersect if and only if

$$z^2+z+1\equiv 0 \pmod p$$

is solvable, in which case there are 2 elements in the intersection. Therefore the double sum in (3.1) is equal to $2(p-2)-(1+(-3/p))=2p-5-(-3/p)$, where $(\cdot/p)$ is the Legendre symbol. This proves the theorem. □

4. The fourth power-moment $W_4(p)$ and proof of Theorem 1.3

Let us denote by $\mathbf{x}$ the vector $(x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4,a)\in(\mathbb{F}_p^*)^9$. Then from (1.12) we have that the fourth moment of $\widetilde{S}(a,1,1;p,p^2)$ is equal to

$$W_4(p)=p^4\sum_{\mathbf{x}\in(\mathbb{F}_p^*)^9}\psi(g(\mathbf{x})),$$

where $\psi(y):=e(y/p)$ is a nontrivial additive character of $\mathbb{F}_p$ and

$$g(\mathbf{x})=a(x_1+x_2+x_3+x_4)+\frac{y_1}{x_1}+\frac{y_2}{x_2}+\frac{y_3}{x_3}+\frac{y_4}{x_4}+\frac{1}{y_1}+\frac{1}{y_2}+\frac{1}{y_3}+\frac{1}{y_4}$$

is a regular function on $(\mathbb{F}_p^*)^9$.

After the change of variables, $ax_i\mapsto x_i$, $1/y_i\mapsto y_i$, for $i=1,2,3,4$, we get that

$$W_4(p)=p^4\sum_{\mathbf{x}\in(\mathbb{F}_p^*)^9}\psi(f(\mathbf{x})),$$

where

$$f(\mathbf{x})=x_1+x_2+x_3+x_4+y_1+y_2+y_3+y_4+\frac{a}{x_1y_1}+\frac{a}{x_2y_2}+\frac{a}{x_3y_3}+\frac{a}{x_4y_4}. \tag{4.1}$$

In the general situation, let us denote an $\mathbb{F}_p$-regular function on the torus $(\mathbb{F}_p^*)^n$ by

$$f(\mathbf{x})=\sum_{j\in J}a_j\mathbf{x}^j\in\mathbb{F}_p[x_1,x_2,\dots,x_n,(x_1,\dots,x_n)^{-1}],$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{x}^j = x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$ and the sum is over a finite subset J of $\mathbb{Z}^n$. Then *the Newton polyhedron* $\Delta(f)$ of $f(\mathbf{x})$ is defined as the convex hull in $\mathbb{R}^n$ of $J \cup \{(0, 0, \ldots, 0)\}$.

With any face (of any dimension) σ of $\Delta(f)$ one associates the corresponding Laurent polynomial

$$f_\sigma = \sum_{j \in \sigma \cap J} a_j \mathbf{x}^j.$$

The function f is said to be *nondegenerate* with respect to its Newton polyhedron $\Delta(f)$, if for every face σ of $\Delta(f)$, not containing the origin, the partial derivatives

$$\frac{\partial f_\sigma}{\partial x_1}, \frac{\partial f_\sigma}{\partial x_2}, \ldots, \frac{\partial f_\sigma}{\partial x_n}$$

have no common zero in $(\overline{\mathbb{F}}_p^*)^n$, where $\overline{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$. Then the following holds:

Theorem 4.1 (Adolphson, Sperber, [1])**.** *For a given n-dimensional polyhedron Δ in $\mathbb{R}^n$ there is a set $\mathcal{S}_\Delta$ which can be effectively determined and which consists of all but finitely many prime numbers, such that for all $p \in \mathcal{S}_\Delta$ and for any regular function*

$$f \in \mathbb{F}_p[x_1, x_2, \ldots, x_n, (x_1, \ldots, x_n)^{-1}]$$

with $\Delta(f) = \Delta$ which is nondegenerate with respect to Δ we have

$$\left| \sum_{\mathbf{x} \in (\mathbb{F}_p^*)^n} \psi(f(\mathbf{x})) \right| \leqslant n!\, V(f) p^{n/2}, \tag{4.2}$$

where $V(f)$ denotes the volume of $\Delta(f)$.

The bound (1.17) will follow immediately from this theorem, if we show that our particular function (4.1) is nondegenerate.

For any face σ of $\Delta(f)$ for which the corresponding Laurent polynomial f_σ has at most two of the terms x_i, y_i, or $a x_i^{-1} y_i^{-1}$ for some $i = 1, 2, 3, 4$, the nondegeneracy condition is trivially satisfied.

Therefore, the only problem can occur if f_σ, for some face σ, is of the form

$$\sum_i \left(x_i + y_i + \frac{a}{x_i y_i} \right),$$

where i runs over some subset of $\{1, 2, 3, 4\}$.

If $f_\sigma = x_i + y_i + a/x_i y_i$, then $\partial f_\sigma / \partial a \neq 0$ everywhere on $(\overline{\mathbb{F}}_p^*)^9$.

If f_σ is of the form $\sum_{i=1}^{2}(x_i + y_i + a/x_i y_i)$, from

$$\frac{\partial f_\sigma}{\partial x_1} = \frac{\partial f_\sigma}{\partial x_2} = \frac{\partial f_\sigma}{\partial y_1} = \frac{\partial f_\sigma}{\partial y_2} = \frac{\partial f_\sigma}{\partial a} = 0,$$

one would get first that $x_1 = y_1$, $x_2 = y_2$ and then also that $x_1^{-2} + x_2^{-2} = 0$ and $x_1^3 = x_2^3$ $(= a)$. But the last two equations have no common solutions in $(\overline{\mathbb{F}}_p^*)^2$, if p is odd.

If $f_\sigma = \sum_{i=1}^{4}(x_i + y_i + a/x_i y_i)$, the system

$$\frac{\partial f_\sigma}{\partial x_1} = \ldots = \frac{\partial f_\sigma}{\partial x_4} = \frac{\partial f_\sigma}{\partial y_1} = \ldots = \frac{\partial f_\sigma}{\partial y_4} = \frac{\partial f_\sigma}{\partial a} = 0$$

leads to $x_i = y_i$ for $i = 1, \ldots, 4$ and then also to $x_1^3 = x_2^3 = x_3^3 = x_4^3$ $(= a)$ and $x_1^{-2} + x_2^{-2} + x_3^{-2} + x_4^{-2} = 0$. This gives the equation

$$1 + \left(\frac{x_1}{x_2}\right)^2 + \left(\frac{x_1}{x_3}\right)^2 + \left(\frac{x_1}{x_4}\right)^2 = 0,$$

where all x_1/x_2, x_1/x_3, x_1/x_4 are the cube roots of unity in $\overline{\mathbb{F}}_p$. By checking all the cases, this has no solutions for all odd primes $p \neq 7$.

In the remaining case, when f_σ is of the form

$$f_\sigma = \sum_{i=1}^{3}\left(x_i + y_i + \frac{a}{x_i y_i}\right), \tag{4.3}$$

the corresponding system of equations actually has solutions on the torus $(\overline{\mathbb{F}}_p^*)^9$. But in this case, σ (that is, the convex hull of the exponents of all monomials occurring in f_σ) is *not* a face of the polyhedron $\Delta(f)$!

To see this, let us denote by $j_1, \ldots, j_4, k_1, \ldots, k_4, l$ the coordinates in the 9-dimensional space in which the Newton polyhedron $\Delta(f)$ is defined. That is, with a monomial $x_1^{j_1} \ldots x_4^{j_4} y_1^{k_1} \ldots y_4^{k_4} a^l$ we associate the lattice point $(j_1, \ldots, j_4, k_1, \ldots, k_4, l)$ in $\mathbb{Z}^9$. Then all the exponents of Laurent polynomial (4.1) lie on the hyperplane

$$j_1 + j_2 + j_3 + j_4 + k_1 + k_2 + k_3 + k_4 + 3l = 1$$

in this 9-space.

The key remark (and the author is grateful to A. Adolphson for pointing out this fact) is that this implies that the faces of $\Delta(f)$ not containing the origin (which are the only faces we need to consider) are exactly the intersections of this hyperplane with the faces of $\Delta(f)$ that do contain the origin.

An arbitrary hyperplane containing the origin is of the form

$$A_1 j_1 + A_2 j_2 + A_3 j_3 + A_4 j_4 + B_1 k_1 + B_2 k_2 + B_3 k_3 + B_4 k_4 + Cl = 0,$$

where $A_1, \ldots, A_4, B_1, \ldots, B_4, C$ are real constants. Let us suppose that this hyperplane contains the lattice points corresponding to the exponents of the monomials in (4.3). This implies first that $A_1 = A_2 = A_3 = B_1 = B_2 = B_3 = 0$ and then further that $C = 0$. Therefore, the only hyperplanes through the origin containing the lattice points corresponding to the monomials from (4.3) will have the form

$$A_4 j_4 + B_4 k_4 = 0.$$

But no such hyperplane can be the support of a face of the Newton polyhedron $\Delta(f)$. Namely, if A_4 and B_4 are not both zero, then $A_4 j_4 + B_4 k_4$ will be positive on one of the lattice points corresponding to the three monomials x_4, y_4 and $ax_4^{-1} y_4^{-1}$, and at the same time, negative on another one of those lattice points. This means that there are vertices of the Newton polyhedron $\Delta(f)$ which lie on opposite sides of this hyperplane. Hence, (4.3) cannot correspond to a face of $\Delta(f)$ not containing the origin, and (4.1) is nondegenerate. $\square$

Acknowledgement. The author is grateful to the referee for useful and constructive comments and suggestions. Also the author is indebted to Professor A. Adolphson for helpful correspondence and for providing an explanation of the results from his joint work [1] with S. Sperber.

References

[1] *A. Adolphson, S. Sperber*: Exponential sums and Newton polyhedra: cohomology and estimates. Ann. Math. (2) *130* (1989), 367–406.

[2] *D. Bump, S. Friedberg, D. Goldfeld*: Poincaré series and Kloosterman sums for $\mathrm{SL}(3, \mathbb{Z})$. Acta Arith. *50* (1988), 31–89.

[3] *D. Goldfeld*: Automorphic Forms and L-Functions for the Group $\mathrm{GL}(n, \mathbb{R})$. With an appendix by Kevin A. Broughan. Cambridge Studies in Advanced Mathematics 99. Cambridge University Press, Cambridge, 2006.

[4] *H. Iwaniec*: Topics in Classical Automorphic Forms. Graduate Studies in Mathematics 17, AMS, Providence, RI, 1997.

[5] *H. D. Kloosterman*: On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. Acta Math. *49* (1927), 407–464.

[6] *M. Larsen*: Appendix to Poincaré series and Kloosterman sums for $\mathrm{SL}(3, \mathbb{Z})$, in The estimation of $SL_3(\mathbb{Z})$ Kloosterman sums. Acta Arith. *50* (1988), 86–89.

Author's address: Goran Djanković, University of Belgrade, Faculty of Mathematics, Studentski Trg 16, p.p. 550, 11000 Belgrade, Serbia, e-mail: djankovic@matf.bg.ac.rs.