Bull. Aust. Math. Soc. (First published online 2025), page 1 of 13*
doi:10.1017/S0004972725100609
*Provisional—final page numbers to be inserted when paper edition is published

SUMS OF KLOOSTERMAN SUMS OVER SQUARE-FREE AND SMOOTH INTEGERS

XUANCHENG SHAO, IGOR E. SHPARLINSKI and LAURENCE P. WIJAYA

(Received 15 July 2025; accepted 12 September 2025)

Abstract

Recently, there has been a large number of works on bilinear sums with Kloosterman sums and on sums of Kloosterman sums twisted by arithmetic functions. Motivated by these, we consider several related new questions about sums of Kloosterman sums parametrised by square-free and smooth integers. Some of our results are presented in the much more general setting of trace functions.

2020 *Mathematics subject classification*: primary 11L05; secondary 11L07, 11N25.

Keywords and phrases: sum of Kloosterman sums, square-free integers, smooth integers.

1. Introduction

1.1. Motivation. For a prime p and an integer n, we define the s-dimensional Kloosterman sum

$$\mathcal{K}_{s,p}(n) = p^{-(s-1)/2} \sum_{\substack{x_1,\ldots,x_s=1 \\ x_1\cdots x_s\equiv n \pmod p}}^{p-1} \mathbf{e}_p(x_1 + \cdots + x_s),$$

where $\mathbf{e}_p(x) = \exp(2\pi i x/p)$. The celebrated result of Deligne [7] gives the bound

$$|\mathcal{K}_{s,p}(n)| \leqslant s. \tag{1.1}$$

(See also [16, Section 11.11].) In the classical case of $s = 2$, we denote

$$\mathcal{K}_p(n) = \mathcal{K}_{2,p}(n).$$

Recently, there has been active interest in estimating sums of Kloosterman sums either over sequences of parameters n of arithmetic interest or twisted by arithmetic functions, such as

During the preparation of this work, X.S. was supported by NSF Grant DMS-2200565 and I.S. was supported in part by ARC Grant DP230100534.

$$P_{s,p}(L) = \sum_{\substack{\ell \leqslant L \\ \ell \text{ prime}}} \mathcal{K}_{s,p}(\ell) \quad \text{and} \quad M_{s,p}(f;N) = \sum_{n \leqslant N} f(n)\mathcal{K}_{s,p}(n), \tag{1.2}$$

with some multiplicative function $f(n)$ such as the Möbius function $\mu(n)$ or the divisor function $\tau(n)$. (See, for example, [5, 8, 18, 21].)

These results rely on recent progress on bounds of bilinear Type-I and Type-II sums with Kloosterman sums (see [2, 4, 5, 8, 17, 19, 20, 22, 23]). In particular, [8, Theorem 1.5] implies power-saving bounds on the sums $P_{s,p}(L)$ given by (1.2) with $L \geqslant p^{3/4+\varepsilon}$ for an arbitrary fixed $\varepsilon > 0$. These bounds have been subsequently improved in [5, Theorem 1.8] in the case of $s = 2$ and for the same range of L.

For the sums $M_{s,p}(f;N)$ given by (1.2), [8, Theorem 1.7] gives power-saving bounds on $M_{s,p}(\mu;N)$, provided that $N \geqslant p^{3/4+\varepsilon}$ for an arbitrary fixed $\varepsilon > 0$. Similar bounds are given by [20, Corollary 1.4] on $M_{s,p}(\tau;N)$, provided that $N \geqslant p^{2/3+\varepsilon}$. These thresholds have both been reduced to $N \geqslant p^{1/2+\varepsilon}$ in [18], however with a logarithmic saving instead of a power saving in the bound.

1.2. Outline of our results

1.2.1. Sums of Kloosterman sums over square-free numbers. We first consider sums of Kloosterman sums over square-free numbers (that is, over numbers which are not divisible by the square of a prime):

$$Q_{s,p}(N) = \sum_{n \leqslant N} |\mu(n)|\mathcal{K}_{s,p}(n) = \sum_{\substack{n \leqslant N \\ n \text{ square-free}}} \mathcal{K}_{s,p}(n). \tag{1.3}$$

The trivial bound

$$Q_{s,p}(N) \ll N \tag{1.4}$$

is implied by (1.1). Our goal is twofold: to obtain a nontrivial bound (possibly with a power saving) for N as small as possible and to have a bound as good as possible for any given N. Our main result in this direction is given by Theorem 2.1, which is proved in Section 4.

A rather straightforward approach (see the remarks following the statement of Theorem 2.1), implies that if $p^{1/2+\varepsilon} \leqslant N \leqslant p$ for an arbitrary fixed $\varepsilon > 0$, then

$$Q_{s,p}(N) \ll N^{1/2}p^{1/4+o(1)}, \tag{1.5}$$

which already improves the trivial bound (1.4) in this range. Our Theorem 2.1 provides a power-saving improvement upon (1.5) for any given N in the range $p^{1/2+\varepsilon} \leqslant N \leqslant p$. For example, if $N = p$, then Theorem 2.1 implies

$$Q_{s,p}(p) \ll p^{3/4-1/232+o(1)}, \tag{1.6}$$

while (1.5) only gives $Q_{s,p}(p) \ll p^{3/4+o(1)}$.

https://doi.org/10.1017/S0004972725100609 Published online by Cambridge University Press

1.2.2. Sums of Kloosterman sums over smooth numbers. Next, we recall that an integer $n \geqslant 1$ is called y-smooth if $P(n) \leqslant y$, where $P(n)$ denotes the largest prime divisor of n. See [13, 15] for background and classical estimates on smooth numbers. For $N \geqslant y \geqslant 2$, we denote by $\mathcal{S}(N, y)$ the set of y-smooth positive integers $n \leqslant N$ and, as usual, we denote $\Psi(N, y) = \#\mathcal{S}(N, y)$.

We consider the sum

$$R_{s.p}(N, y) = \sum_{n \in \mathcal{S}(N,y)} \mathcal{K}_{s,p}(n),$$

for which we have, in analogy to (1.4), the trivial bound

$$R_{s,p}(N, y) \ll \Psi(N, y) \leqslant N.$$

As in the case of squarefree numbers, our goal is to obtain nontrivial bounds for N as small as possible and, at the same time, to have a bound as good as possible for any given N and y. Additionally, we are also interested in obtaining nontrivial bounds for y as small as possible.

In fact, it turns out that the estimates we have for $R_{s,p}(N, y)$ hold in a much broader context of trace functions (see Section 1.3). Thus, given a trace function $\mathsf{K}(n)$, we consider the generalisation of $R_{s,p}(N, y)$,

$$R_{\mathsf{K}}(N, y) = \sum_{n \in \mathcal{S}(N,y)} \mathsf{K}(n), \tag{1.7}$$

for which, if the values of $\mathsf{K}(n)$ are uniformly bounded, we have, in analogy to (1.4), the trivial bound

$$R_{\mathsf{K}}(N, y) \ll \Psi(N, y) \leqslant N.$$

Our main result in this direction is given by Theorem 2.2, which is proved in Section 4. As a special case of Theorem 2.2, if $\log y/\log\log N \to \infty$, then

$$R_{\mathsf{K}}(N, y) \ll \Psi(N, y) y^{1/2} p^{1/8} N^{-1/4+o(1)}, \tag{1.8}$$

which is nontrivial when $N > y^2 p^{1/2+\varepsilon}$. (See the remarks following the statement of Theorem 2.2.)

1.3. Trace functions. Many of the results that are mentioned in Section 1.1 also apply to more general sums involving *trace functions* (apart from several exceptions described in [5, 17, 20–23]). The exact definition of these trace functions requires some notions from algebraic geometry, which go beyond the more analytic frameworks of this work. Instead, we refer to [8–10] and especially [11] for a general background, and precise definitions and properties of trace functions.

It turns out that Kloosterman sums are representatives of a much richer class of *isotypic trace functions* $\mathsf{K}(n)$, which are associated with isotypic trace sheaves $\mathfrak{F}$ modulo p of bounded conductor (we refer to [8, 9] for precise definitions and properties

https://doi.org/10.1017/S0004972725100609 Published online by Cambridge University Press

of trace functions). In addition to Kloosterman sums, other concrete examples of isotypic trace functions include:

- traces of Frobenius of elliptic curves modulo p;
- exponential functions of the form $\mathbf{e}(\psi(n)/p)$ with rational functions $\psi(Z) \in \mathbb{Q}(Z)$ and similar values of multiplicative characters as well as their products.

Some of our principal tools, such as Lemmas 3.1 and 3.2 below, are presented for trace functions. Because of these observations, in Theorem 2.2, we present a bound on $R_{\mathsf{K}}(N, y)$ for a large class of trace functions, including Kloosterman sums, rather than a bound on just $R_{s,p}(N, y)$.

However, the main ingredient in the proof of Theorem 2.1, Lemma 3.3, is based on [20, Theorem 4.3], which, at the moment, is only known for Kloosterman sums. Thus, it is not clear how to extend Theorem 2.1 to arbitrary trace functions (though an analogue of the trivial bound (1.5) still holds).

1.4. Structure of the paper. The rest of the paper is organised as follows. In Section 2, we formulate our main results, and also show how the bounds (1.6) and (1.8) follow from them. Then, in Section 3.2, we state some preliminary results including estimates for sums of trace functions and a variant of the Type-I estimate for Kloosterman sums, which are crucial in our treatment of smooth numbers and square-free numbers. Then, in Section 4, we prove Theorems 2.1 and 2.2.

2. Main results

2.1. Sums of Kloosterman sums over square-free numbers. Our main result in this direction is the following bound. Recall the definition of $Q_{s,p}(N)$ from (1.3).

THEOREM 2.1. *For any positive integer $s \geqslant 2$ and any even positive integer ℓ, if $p^{1/2+2/\ell} \leqslant N \leqslant p$, then*

$$|Q_{s,p}(N)| \leqslant N^{1/2} p^{1/4} \left(\frac{p^{1/2+2/\ell}}{N}\right)^{1/2(4\ell-3)} p^{o(1)}.$$

For a specific value of N, one can optimise the bound in Theorem 2.1 by making the choice of ℓ that minimises the term

$$\left(\frac{p^{1/2+2/\ell}}{N}\right)^{1/2(4\ell-3)}.$$

For example, if $N = p$, then by choosing $\ell = 8$, we derive (1.6). We also note that the bound (1.5) can be quickly obtained by combining (4.1) and (4.2) in our proof of Theorem 2.1.

Our approach works for $N > p$ as well. However, the optimisation of our argument becomes more cluttered in such generality. Since we are mostly interested in short sums and to exhibit our ideas in the simplest possible form, we focus on the case $N \leqslant p$.

2.2. Sums of trace function over smooth numbers. Before formulating our main result in this direction, we recall some well-known estimates in the theory of smooth numbers. Let $\alpha(N,y)$ be the *saddle point* corresponding to the y-smooth numbers up to N as discussed in [14, 15]. In particular, $\alpha(N,y)$ satisfies

$$\alpha(N,y) = (1+o(1))\frac{\log(1+y/\log N)}{\log y},$$

provided that $y \le N$ and $y \to \infty$ (see [15, Theorem 2]). In particular, if $\log y/\log\log N \to \infty$, then $\alpha(N,y) \to 1$ and if $y = (\log N)^K$ for some $K \ge 1$, then $\alpha(N,y) = 1 - 1/K + o(1)$. We have

$$\Psi(N,y) = N^{\alpha(N,y)+o(1)} \tag{2.1}$$

(see, for example, [14, Section 2] or [15, Theorem 1]).

Our main result in this direction is the following bound. Recall the definition of $R_{\mathsf{K}}(N,y)$ from (1.7).

THEOREM 2.2. *Let* K *be a nonexceptional isotypic trace function associated to some sheaf* $\mathfrak{F}$ *modulo a prime* p *of bounded conductor. For* $N \ge p^{1/2}$ *and* $y \ge \log N$,

$$|R_{\mathsf{K}}(N,y)| \leqslant \Psi(N,y)y^{1/2}p^{\beta}N^{-\gamma+o(1)},$$

where

$$\beta = \frac{1}{4(1+\alpha(N,y))} \quad \textit{and} \quad \gamma = \frac{\alpha(N,y)^2}{2(1+\alpha(N,y))}.$$

Some remarks on the bound are in order. If $y = N^{o(1)}$, then $y^{1/2}$ can be dropped from the bound giving

$$R_{\mathsf{K}}(N,y) \ll \Psi(N,y)p^{\beta}N^{-\gamma+o(1)},$$

which is nontrivial when $N \geqslant p^{\beta/\gamma+\varepsilon} = p^{1/2\alpha(N,y)^2+\varepsilon}$ for arbitrary fixed $\varepsilon > 0$. In the special case $N = p$, we have a nontrivial bound for $R_{\mathsf{K}}(N,y)$, provided that $\alpha(N,y) > 1/\sqrt{2}$ or $y \ge (\log N)^{2+\sqrt{2}+\varepsilon}$.

However, if $\log y/\log\log N \to \infty$, then $\alpha(N,y) = 1 + o(1)$. Hence, $\beta = 1/8 + o(1)$ and $\gamma = 1/4 + o(1)$. Thus, Theorem 2.2 yields (1.8).

3. Preparations

3.1. Notation. We use the standard notation $U \ll V$ and $V \gg U$ as equivalent to the statement $|U| \le cV$, for some constant $c > 0$, which, throughout this paper, may depend only on the integer parameters ℓ and s.

For a finite set $\mathcal{S}$, we use $\#\mathcal{S}$ to denote its cardinality.

The variables of summation d, k, m and n are always positive integers.

We also follow the convention that fractions of the shape $1/ab$ mean $1/(ab)$ (rather than b/a as their formal interpretation might suggest).

https://doi.org/10.1017/S0004972725100609 Published online by Cambridge University Press

The letter p always denotes a prime number and we use $\mathbb{F}_p$ to denote the finite field of p elements.

We denote by $p(\ell)$ and $P(\ell)$ the smallest and the largest prime factors of an integer $\ell \neq 0$, respectively. We adopt the convention that $p(1) = P(1) = +\infty$.

Finally, we write $\sum_{k \leqslant K}$ to denote the summation over positive integers $k \leqslant K$.

3.2. Preliminary bounds on sums of trace functions and Kloosterman sums. We recall the following bound, which is a combination of [8, Proposition 6.2] and [8, Theorem 6.3] (see [10–12] for several other variations of this result).

LEMMA 3.1. *Let* K *be a nonexceptional isotypic trace function associated to some sheaf* $\mathfrak{F}$ *modulo a prime* p *of bounded conductor. There exists a set* $\mathcal{E}_{\mathfrak{F}} \subseteq \mathbb{F}_p$ *of cardinality* $\#\mathcal{E}_{\mathfrak{F}} \ll 1$*, such that uniformly over* $d \in \mathbb{F}_p \setminus \mathcal{E}_{\mathfrak{F}}$ *and* $h \in \mathbb{Z}$*,*

$$\sum_{x \in \mathbb{F}_p} \mathsf{K}(x)\mathsf{K}(dx)\,\mathbf{e}_p(hx) \ll p^{1/2}.$$

The standard completion technique (see [16, Section 12.2]) shows that Lemma 3.1 implies the following bound on incomplete sums.

LEMMA 3.2. *In the notation of Lemma 3.1, for any* $K \leqslant p$*, uniformly over* $d, e \in \mathbb{F}_p$ *satisfying* $d \neq 0$ *and* $e/d \notin \mathcal{E}_{\mathfrak{F}}$*,*

$$\sum_{n \leqslant K} \mathsf{K}(dn)\mathsf{K}(en) \ll p^{1/2} \log p.$$

Furthermore, only in the case of Kloosterman sums, we need the following estimate of the *Pólya–Vinogradov* type: for any $K \leqslant p$, uniformly over $d \in \mathbb{F}_p^*$,

$$\sum_{n \leqslant K} \mathcal{K}_{s,p}(dn) \ll p^{1/2} \log p. \tag{3.1}$$

(See [11, Theorem 6.2]. The result also follows from [10, Corollary 1.6] and the completion techniques of [16, Section 12.2].)

We now record a bound on a variant of Type-I sums of Kloosterman sums. Instead of Type-I sums with $\mathcal{K}_{s,p}(mn)$, we consider sums with $\mathcal{K}_{s,p}(m^r n)$, where r is an arbitrary integer (if r is negative, we consider the argument of the corresponding Kloosterman sum modulo p). This is obtained by a slight extension of the argument of [20]. As we have mentioned, this result does not immediately extend to general trace functions. (See [3, 4, 8, 17, 19, 20] for several other bounds on related sums.)

LEMMA 3.3. *Fix an integer* $r \neq 0$ *and an even integer* $\ell \geqslant 2$*. Let* $D, N \leqslant p$ *be positive integers with* $N > 2p^{1/\ell}$*. For each* $d \leqslant D$*, let* $\mathcal{N}_d \subseteq [1, N]$ *be an interval. Then, for any complex weights* $\boldsymbol{\alpha} = \{\alpha_d\}_{d \leqslant D}$ *with* $\alpha_d \ll 1$*,*

$$\sum_{d \leqslant D} \sum_{n \in \mathcal{N}_d} \alpha_d \mathcal{K}_{s,p}(d^r n) \ll DN\Big(N^{-1} + \frac{p^{1+1/\ell}}{DN^2}\Big)^{1/(2\ell)} p^{o(1)}.$$

https://doi.org/10.1017/S0004972725100609 Published online by Cambridge University Press

PROOF. We follow the proof of [20, Theorem 4.3], which is conveniently summarised in [3, Section 4.3] and also extended to sums when the nonsmooth variable runs through an arbitrary set. Let

$$S = \sum_{d\leqslant D}\sum_{n\in\mathcal{N}_d}\alpha_d\mathcal{K}_{s,p}(d^r n).$$

Let A and B be integer parameters to be chosen later for which

$$2AB \leqslant N. \tag{3.2}$$

By introducing averages over $a \sim A$ and $b \sim B$ (where $a \sim A$ denotes the dyadic range $A \le a < 2A$ and similarly for $b \sim B$), and replacing n by $n + ab$,

$$\begin{aligned} S &= \frac{1}{AB}\sum_{a\sim A}\sum_{b\sim B}\sum_{d\le D}\alpha_d \sum_{\substack{n\in\mathbb{Z}\\ n+ab\in\mathcal{N}_d}}\mathcal{K}_{s,p}(d^r(n+ab))\\ &= \frac{1}{AB}\sum_{a\sim A}\sum_{d\le D}\alpha_d\sum_{n\in\mathbb{Z}}\sum_{\substack{b\sim B\\ n+ab\in\mathcal{N}_d}}\mathcal{K}_{s,p}(d^r(n+ab)). \end{aligned}$$

Since the range for the inner sum over b is an interval, by the completion technique (see [16, Section 12.2]),

$$S \ll \frac{\log p}{AB}\sum_{a\sim A}\sum_{d\le D}\sum_{n=-N}^{N}\Big|\sum_{b\sim B}\mathcal{K}_{s,p}(d^r(n+ab))\,\mathbf{e}(bt)\Big|$$

for some $t \in \mathbb{R}$, where $\mathbf{e}(z) = \exp(2\pi i z)$. By making a change of variables $u = d^r a$ and $v = \overline{a}n$,

$$S \ll \frac{\log p}{AB}\sum_{u,v\in\mathbb{F}_p}\nu(u,v)\Big|\sum_{b\sim B}\mathcal{K}_{s,p}(u(v+b))\,\mathbf{e}(bt)\Big|,$$

where $\nu(u,v)$ is the number of triples (a,m,n) with $a \sim A$, $m \in \{d^r : 1 \le d \le D\}$ and $n \in [-N, N]$ such that

$$u \equiv \overline{a}n \pmod p \quad \text{and} \quad v \equiv ma \pmod p.$$

Following the steps in [3, Section 4.3] leading to [3, (4.9), (4.10) and (4.11)] and defining $\mathcal{M} = \{d^r : 1 \le d \le D\}$,

$$S^{2\ell} \ll A^{-2}B^{-2\ell}D^{2\ell-2}N^{2\ell-1}(B^\ell p^2 + B^{2\ell}p)J(2A,\mathcal{M})p^{o(1)}, \tag{3.3}$$

where $J(H,\mathcal{M})$ denotes the number of solutions to the congruence

$$xk \equiv ym \bmod p \tag{3.4}$$

for which $x, y \in [1, H]$ and $k, m \in \mathcal{M}$. Taking $B = \lfloor p^{1/\ell}\rfloor$, we see that (3.3) simplifies as

$$S^{2\ell} \ll A^{-2}D^{2\ell-2}N^{2\ell-1}J(2A,\mathcal{M})p^{1+o(1)}. \tag{3.5}$$

In the setting of the proof of [20, Theorem 4.3], the condition

$$2A \max_{m \in \mathcal{M}} m < p \tag{3.6}$$

is satisfied, which allows us to replace (3.4) with an equation $xk = ym$ in integers. Then, using the classical bound on the divisor function (see [16, (1.81)]), it is shown in [20] that, under the condition (3.6), we have $J(2A, \mathcal{M}) \leqslant (A\#\mathcal{M})^{1+o(1)}$. However, (3.6) is too restrictive for our purpose, so we instead use a result of Ayyad, Cochrane and Zheng [1, Theorem 2] which, similarly to the proof of [6, Theorem 4.1], leads to the bound

$$J(2A, \mathcal{M}) \ll A^2D^2/p + (AD)^{1+o(1)}. \tag{3.7}$$

Substituting (3.7) in (3.5),

$$S^{2\ell} \ll (D^{2\ell}N^{2\ell-1} + A^{-1}D^{2\ell-1}N^{2\ell-1}p)p^{o(1)}.$$

Since $N > 2p^{1/\ell} \geqslant 2B$, we may choose

$$A = \left\lfloor \frac{N}{2B} \right\rfloor \gg Np^{-1/\ell},$$

which guarantees that the condition (3.2) is met. We obtain the stated bound after simple calculations. □

4. Proofs of the main results

PROOF OF THEOREM 2.1. Using inclusion–exclusion, we can write

$$Q_{s,p}(N) = \sum_{d \leqslant N^{1/2}} \mu(d) \sum_{n \leqslant N/d^2} \mathcal{K}_{s,p}(d^2n).$$

Next, we split the sum $Q_{s,p}(N)$ into dyadic intervals with respect to some parameter $D \geqslant 1$ to get $O(\log N)$ sums of the type

$$S(D, N) = \sum_{d \sim D} \mu(d) \sum_{n \leqslant N/d^2} \mathcal{K}_{s,p}(d^2n)$$

for some $D \leqslant N^{1/2}$. By (3.1),

$$S(D, N) \ll Dp^{1/2} \log p. \tag{4.1}$$

By the Deligne bound (1.1),

$$S(D, N) \ll DN/D^2 = N/D. \tag{4.2}$$

However, for any fixed even integer $\ell > 0$, by Lemma 3.3,

$$S(D, N) \ll DK\left(K^{-1} + \frac{p^{1+1/\ell}}{DK^2}\right)^{1/(2\ell)} p^{o(1)},$$

where $K = N/D^2$, provided that $K > 2p^{1/\ell}$. Note that $DK = N/D \leqslant N \leqslant p \leqslant p^{1+1/\ell}$ and thus,

$$K^{-1} \leqslant \frac{p^{1+1/\ell}}{DK^2}.$$

It follows that if $K > 2p^{1/\ell}$, then

$$S(D,N) \ll DK\Big(\frac{p^{1+1/\ell}}{DK^2}\Big)^{1/(2\ell)} p^{o(1)} = \frac{N}{D}\Big(\frac{D^3 p^{1+1/\ell}}{N^2}\Big)^{1/(2\ell)} p^{o(1)}. \tag{4.3}$$

Using the bounds (4.1) or (4.3) for $K > 2p^{1/\ell}$ and the bound (4.2) for $K \le 2p^{1/\ell}$, we arrive at

$$S(D,N) \ll \min\{f_1(D), f_2(D)\}p^{o(1)} + N^{1/2}p^{1/(2\ell)}, \tag{4.4}$$

where

$$f_1(D) = Dp^{1/2} \quad \text{and} \quad f_2(D) = \frac{N}{D}\Big(\frac{D^3 p^{1+1/\ell}}{N^2}\Big)^{1/(2\ell)}.$$

Choose the parameter

$$D_0 = \Big(\frac{N^{2\ell-2}}{p^{\ell-1-1/\ell}}\Big)^{1/(4\ell-3)} = N^{1/2}p^{-1/4}\Big(\frac{p^{1/2+2/\ell}}{N}\Big)^{1/2(4\ell-3)}$$

such that $f_1(D_0) = f_2(D_0)$. Clearly, $1 \leqslant D_0 \leqslant N^{1/2}$ since $N \geq p^{1/2+2/\ell}$ by assumption. Hence,

$$\min\{f_1(D), f_2(D)\} \leqslant f_1(D_0) \leqslant N^{1/2}p^{1/4}\Big(\frac{p^{1/2+2/\ell}}{N}\Big)^{1/2(4\ell-3)}.$$

It can be easily verified that

$$p^{1/2\ell} \leqslant p^{1/4}\Big(\frac{p^{1/2+2/\ell}}{p}\Big)^{1/2(4\ell-3)} \leqslant p^{1/4}\Big(\frac{p^{1/2+2/\ell}}{N}\Big)^{1/2(4\ell-3)}.$$

Hence, the second term on the right-hand side of (4.4) is dominated by the first term, and

$$S(D,N) \ll N^{1/2}p^{1/4}\Big(\frac{p^{1/2+2/\ell}}{N}\Big)^{1/2(4\ell-3)} p^{o(1)}.$$

This concludes the proof. □

PROOF OF THEOREM 2.2. Let $L_0 \in [1,N]$ be a parameter to be chosen later. Observe that any y-smooth integer in $(L_0, N]$ can be uniquely factored as $n = \ell m$ such that

$$\ell \in (L_0, yL_0], \quad \frac{\ell}{P(\ell)} \le L_0, \quad p(m) \geq P(\ell),$$

where $P(\ell)$ denotes the largest prime factor of ℓ and $p(m)$ denotes the smallest prime factor of m. Indeed, this factorisation can be obtained by writing $n = p_1p_2\cdots p_k$ with primes $p_1 \leqslant \cdots \leqslant p_k$ and by setting $\ell = p_1p_2\cdots p_r$, where r is the smallest positive integer such that $p_1p_2\cdots p_r > L_0$.

https://doi.org/10.1017/S0004972725100609 Published online by Cambridge University Press

Thus,

$$R_{\mathsf{K}}(N,y) = \sum_{\substack{L_0<\ell\le P(\ell)L_0\\ \ell\in S(y)}} \sum_{\substack{m\in\mathcal{S}(N/\ell,y)\\ p(m)\ge P(\ell)}} \mathsf{K}(\ell m) + O(L_0).$$

After dyadic partition of the range for ℓ, we see that there is $L\in(L_0, yL_0]$ such that

$$R_{\mathsf{K}}(N,y) \ll U\log N + L_0, \tag{4.5}$$

where

$$U = \sum_{\substack{L<\ell\le\min\{P(\ell)L_0,2L\}\\ \ell\in S(y)}} \sum_{\substack{m\in\mathcal{S}(N/\ell,y)\\ p(m)\ge P(\ell)}} \mathsf{K}(\ell m).$$

We now employ the completion technique as in [16, Section 12.2] again. That is, first, we write

$$U = \sum_{\substack{L<\ell\le\min\{P(\ell)L_0,2L\}\\ \ell\in S(y)}} \sum_{\substack{m\in\mathcal{S}(N/L,y)\\ p(m)\ge P(\ell)}} \mathsf{K}(\ell m)\frac{1}{N}\sum_{1\leqslant k\leqslant N/\ell}\sum_{a=1}^{N}\mathbf{e}(a(m-k)/N),$$

where, as before, $\mathbf{e}(z)=\exp(2\pi i z)$. After changing the order of summation and using [16, (8.6)] (similarly to the argument in Section 4), we derive

$$U \ll \sum_{\substack{\ell\sim L\\ \ell\in S(y)}} \Bigg|\sum_{\substack{m\in\mathcal{S}(N/L,y)\\ p(m)\ge P(\ell)}} \mathsf{K}(\ell m)\,\mathbf{e}(\eta m)\Bigg| \log N$$

for some real $\eta\in\mathbb{R}$.

By the Cauchy–Schwarz inequality,

$$U^2 \ll (\log N)^2\Psi(L,y)\sum_{\substack{\ell\sim L\\ \ell\in S(y)}} \Bigg|\sum_{\substack{m\in\mathcal{S}(N/L,y)\\ p(m)\ge P(\ell)}} \mathsf{K}(\ell m)\,\mathbf{e}(\eta m)\Bigg|^2.$$

Writing $q=P(\ell)$ and replacing ℓ by $q\ell$,

$$U^2 \ll (\log N)^2\Psi(L,y)\sum_{q\le y}\sum_{\ell\sim L/q} \Bigg|\sum_{\substack{m\in\mathcal{S}(N/L,y)\\ p(m)\ge q}} \mathsf{K}(q\ell m)\,\mathbf{e}(\eta m)\Bigg|^2,$$

where we have dropped the primality condition on q. Expanding the square,

$$U^2 \ll (\log N)^2\Psi(L,y)\sum_{q\le y}\sum_{m_1,m_2\in\mathcal{S}(N/L,y)} \Bigg|\sum_{\ell\sim L/q}\mathsf{K}(q\ell m_1)\overline{\mathsf{K}(q\ell m_2)}\Bigg|. \tag{4.6}$$

https://doi.org/10.1017/S0004972725100609 Published online by Cambridge University Press

The contribution Y_1 to the right-hand side of (4.6) from terms with $m_1/m_2 \in \mathcal{E}_{\mathfrak{F}}$ is

$$Y_1 \ll (\log N)^2 \Psi(L, y) \sum_{q \le y} \Psi(N/L, y) \frac{L}{q} \ll LN^{-\alpha} \Psi(N, y)^2 (\log N)^3,$$

where $\alpha = \alpha(N, y)$ and we have also used the standard bounds (see [14, Section 2])

$$\Psi(L, y) \ll \Big(\frac{L}{N}\Big)^{\alpha} \Psi(N, y), \quad \Psi(N/L, y) \ll \frac{1}{L^{\alpha}} \Psi(N, y).$$

To estimate the contribution Y_2 to the right-hand side of (4.6) from terms with $m_1/m_2 \notin \mathcal{E}_{\mathfrak{F}}$, we observe that Lemma 3.2 implies that

$$\Big| \sum_{\ell \sim L/q} \mathsf{K}(q\ell m_1) \overline{\mathsf{K}(q\ell m_2)} \Big| \ll p^{1/2} \log p$$

when $m_1/m_2 \notin \mathcal{E}_{\mathfrak{F}}$. Hence,

$$Y_2 \ll (\log N)^2 \Psi(L, y) \cdot y \Psi(N/L, y)^2 p^{1/2} \log p \ll y p^{1/2} L^{-\alpha} \Psi(N, y)^2 N^{o(1)}.$$

Overall, with $\alpha = \alpha(N, y)$, then,

$$\begin{aligned} U^2 &\ll Y_1 + Y_2 \leqslant (LN^{-\alpha} + yp^{1/2} L^{-\alpha}) \Psi(N, y)^2 N^{o(1)} \\ &\leqslant y(L_0 N^{-\alpha} + p^{1/2} L_0^{-\alpha}) \Psi(N, y)^2 N^{o(1)}. \end{aligned}$$

Choosing $L_0 = p^{1/2(1+\alpha)} N^{\alpha/(1+\alpha)}$ to balance the two terms depending on L_0, we conclude that

$$U \leqslant y^{1/2} p^{1/4(1+\alpha)} N^{-\alpha^2/2(1+\alpha)} \Psi(N, y) N^{o(1)}.$$

Hence, we see from (4.5) that

$$\begin{aligned} R_{\mathsf{K}}(N, y) &\ll \Psi(N, y) y^{1/2} p^{1/4(1+\alpha)} N^{-\alpha^2 2(1+\alpha)+o(1)} + p^{1/2(1+\alpha)} N^{\alpha/(1+\alpha)} \\ &= \Psi(N, y) y^{1/2} p^{\beta} N^{-\gamma+o(1)} + p^{2\beta} N^{\alpha-2\gamma}. \end{aligned}$$

We may assume that $p^{\beta} \leqslant N^{\gamma}$ since otherwise, the claimed bound is trivial. Using (2.1),

$$p^{2\beta} N^{\alpha-2\gamma} \leqslant p^{\beta} N^{\alpha-\gamma} = \Psi(N, y) p^{\beta} N^{-\gamma+o(1)}$$

and the result follows. □

Acknowledgement

The authors would like to thank the referee for very encouraging comments.

References

[1] A. Ayyad, T. Cochrane and Z. Zheng, ‘The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$ and the mean values of character sums’, *J. Number Theory* **59** (1996), 398–413.

[2] N. Bag and I. E. Shparlinski, ‘Bounds on bilinear sums of Kloosterman sums’, *J. Number Theory* **242** (2023), 102–111.

[3] W. Banks and I. E. Shparlinski, ‘Congruences with intervals and arbitrary sets’, *Arch. Math.* **114** (2020), 527–539.

https://doi.org/10.1017/S0004972725100609 Published online by Cambridge University Press

[4] V. Blomer, É. Fouvry, E. Kowalski, P. Michel and D. Milićević, 'On moments of twisted L-functions', *Amer. J. Math.* **139** (2017), 707–768.

[5] V. Blomer, É. Fouvry, E. Kowalski, P. Michel and D. Milićević, 'Some applications of smooth bilinear forms with Kloosterman sums', *Tr. Mat. Inst. Steklova* **296** (2017), 24–35; English translation in *Proc. Steklov Inst. Math.* **296** (2017), 18–29.

[6] J. Cilleruelo, I. E. Shparlinski and A. Zumalacárregui, 'Isomorphism classes of elliptic curves over a finite field in some thin families', *Math. Res. Lett.* **9** (2012), 335–343.

[7] P. Deligne, *Cohomologie Étale (SGA* $4\frac{1}{2}$*)*, Lecture Notes in Mathematics, 569 (Springer-Verlag, Berlin, 1977).

[8] É. Fouvry, E. Kowalski and P. Michel, 'Algebraic trace functions over the primes', *Duke Math. J.* **163** (2014), 1683–1736.

[9] É. Fouvry, E. Kowalski and P. Michel, 'Trace functions over finite fields and their applications', in: *Colloquium De Giorgi 2013 and 2014* (ed. U. Zannier), Publications of the Scuola Normale Superiore, 5 (Edizioni della Normale, Pisa, 2015), 7–35.

[10] É. Fouvry, E. Kowalski and P. Michel, 'A study in sums of products', *Philos. Trans. Roy. Soc. A* **373** (2015), 20140309.

[11] É. Fouvry, E. Kowalski and P. Michel, 'Lectures on applied ℓ-adic cohomology', in: *Analytic Methods in Arithmetic Geometry*, Contemporary Mathematics, 740 (eds. A. Bucur and D. Zureick-Brown) (American Mathematical Society, Providence, RI, 2019), 113–195.

[12] É. Fouvry, E. Kowalski, P. Michel, C. S. Raju, J. Rivat and K. Soundararajan, 'On short sums of trace functions', *Ann. Inst. Fourier (Grenoble)* **167** (2017), 423–449.

[13] A. Granville, 'Smooth numbers: computational number theory and beyond', in: *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, Publications of the Research Institute for Mathematical Sciences, 44 (eds. J. P. Buhler and P. Stevenhagen) (Cambridge University Press, Cambridge, 2008), 267–324.

[14] A. J. Harper, 'Minor arcs, mean values, and restriction theory for exponential sums over smooth numbers', *Compos. Math.* **152** (2016), 1121–1158.

[15] A. Hildebrand and G. Tenenbaum, 'Integers without large prime factors', *J. Théor. Nombres Bordeaux* **5** (1993), 411–484.

[16] H. Iwaniec and E. Kowalski, *Analytic Number Theory* (American Mathematical Society, Providence, RI, 2004).

[17] B. Kerr, I. E. Shparlinski, X. Wu and P. Xi, 'Bounds on bilinear forms with Kloosterman sums', *J. Lond. Math. Soc. (2)* **108** (2023), 578–621.

[18] M. Korolev and I. E. Shparlinski, 'Sums of algebraic trace functions twisted by arithmetic functions', *Pacific J. Math.* **304** (2020), 505–522.

[19] E. Kowalski, P. Michel and W. Sawin, 'Bilinear forms with Kloosterman sums and applications', *Ann. of Math. (2)* **186** (2017), 413–500.

[20] E. Kowalski, P. Michel and W. Sawin, 'Stratification and averaging for exponential sums: bilinear forms with generalized Kloosterman sums', *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)* **21** (2020), 1453–1530.

[21] K. Liu, I. E. Shparlinski and T. P. Zhang, 'Cancellations between Kloosterman sums modulo a prime power with prime arguments', *Mathematika* **65** (2019), 475–487.

[22] I. E. Shparlinski, 'On sums of Kloosterman and Gauss sums', *Trans. Amer. Math. Soc.* **371** (2019), 8679–8697.

[23] I. E. Shparlinski and T. P. Zhang, 'Cancellations amongst Kloosterman sums', *Acta Arith.* **176** (2016), 201–210.

XUANCHENG SHAO, Department of Mathematics,
University of Kentucky, Lexington, USA
e-mail: xuancheng.shao@uky.edu

https://doi.org/10.1017/S0004972725100609 Published online by Cambridge University Press

IGOR E. SHPARLINSKI, School of Mathematics and Statistics,
University of New South Wales, Sydney, New South Wales 2052, Australia
e-mail: igor.shparlinski@unsw.edu.au

LAURENCE P. WIJAYA, Department of Mathematics,
University of Kentucky, Lexington, USA
e-mail: laurence.wijaya@uky.edu

https://doi.org/10.1017/S0004972725100609 Published online by Cambridge University Press