AVERAGE BOUNDS FOR KLOOSTERMAN SUMS OVER PRIMES

Alastair J. Irving

Abstract: We prove two estimates for averages of sums of Kloosterman fractions over primes. The first of these improves previous results of Fouvry-Shparlinski and Baker.

Keywords: Kloosterman sums, sums over primes.

1. Introduction

In this paper we consider bounds for sums of the form

$$S_q(a;x) = \sum_{\substack{p \sim x \\ (p,q)=1}} e\left(\frac{a\overline{p}}{q}\right)$$

where p runs over primes and $u \sim v$ denotes the inequality $v \leqslant u < 2v$. These sums may be bounded trivially by x. If $(a,q) = 1$ then we conjecture that for any $\epsilon > 0$ a bound of

$$S_q(a;x) \ll_\epsilon x^{\frac{1}{2}+\epsilon} q^\epsilon$$

should be true. This conjecture, however, seems to be far out of reach of current methods.

A bound for $S_q(a;x)$ is given by Garaev, [5], in the case that q is prime. He shows that for $x < q$ we have, for any $\epsilon > 0$,

$$\max_{(a,q)=1} |S_q(a;x)| \ll_\epsilon (x^{\frac{15}{16}} + x^{\frac{2}{3}} q^{\frac{1}{4}}) q^\epsilon.$$

This gives us a nontrivial estimate for the sum provided that $x \geqslant q^{\frac{3}{4}+\delta}$ for some $\delta > 0$. For $q \geqslant x \geqslant q^{\frac{16}{17}+\delta}$ Garaev uses this bound to prove an asymptotic for the number of prime solutions, p_1, p_2, p_3 with $p_i \in [0, x]$, to the congruence

$$p_1(p_2 + p_3) \equiv \lambda \pmod{q}.$$

Fouvry and Shparlinski, [4], generalise Garaev's bound to arbitrary q and the larger range $q^{\frac{3}{4}} \leqslant x \leqslant q^{\frac{4}{3}}$. They also show that if we average over q then a sharper bound is possible. Specifically, their Theorem 5 states that if $Q^{\frac{3}{2}} \geqslant x \geqslant 2$ then for every $\epsilon > 0$ we have

$$\sum_{q \sim Q} \max_{(a,q)=1} |S_q(a;x)| \ll_\epsilon (Q^{\frac{13}{10}} x^{\frac{3}{5}} + Q^{\frac{13}{12}} x^{\frac{5}{6}}) Q^\epsilon. \tag{1}$$

This bound is nontrivial when $x \geqslant Q^{\frac{3}{4}+\delta}$. Fouvry and Shparlinski use their estimates to study multiplicative properties of the set

$$\{p_1 p_2 + p_1 p_3 + p_2 p_3 : p_i \sim x, p_i \text{ prime}\}.$$

They show, for example, that for x sufficiently large this set contains numbers with a prime factor exceeding $x^{1.10028}$. Baker, [1, Theorem 2], has recently improved the bound (1) in the range $Q^{\frac{1}{2}} \leqslant x \leqslant 2Q$. His result is

$$\sum_{q \sim Q} \max_{(a,q)=1} |S_q(a;x)| \ll_\epsilon (Q^{\frac{11}{10}} x^{\frac{4}{5}} + Qx^{\frac{11}{12}}) Q^\epsilon. \tag{2}$$

This is nontrivial for $Q \geqslant x^{\frac{1}{2}+\delta}$ and sharper than (1) when $x \leqslant Q^{1-\delta}$. Baker applies this bound to the same ternary form problem as Fouvry and Shparlinski; combining it with a variant on the sieve argument he improves 1.10028 to 1.1673.

We are motivated by a new application of these sums to Diophantine approximation. For this application we need only consider average bounds. We will show that by generalising the arguments from [4] it is possible to obtain a sharper estimate than that given in (1).

Theorem 1.1. *For any $\epsilon > 0$ we have*

$$\sum_{q \sim Q} \max_{(a,q)=1} |S_q(a;x)| \ll_\epsilon (Q^{\frac{5}{4}} x^{\frac{5}{8}} + Qx^{\frac{9}{10}} + Q^{\frac{7}{6}} x^{\frac{13}{18}}) Q^\epsilon$$

for $Q^{\frac{3}{2}} \geqslant x \geqslant Q^{\frac{2}{3}}$.

This gives us a nontrivial result for $x \geqslant Q^{\frac{2}{3}+\delta}$. The proof uses similar methods to those of Fouvry and Shparlinski. However we introduce higher moments into one of their estimates. This results in a problem of counting solutions to a congruence with a larger number of variables; one which we can solve with a sharp bound when we average over q.

Using this theorem we give a further improvement of the exponent in the ternary form problem. Let $P^+(n)$ denote the largest prime factor of n.

Theorem 1.2. *Let $\theta_1 = 1.188\ldots$ be the unique root of the equation*

$$42\theta - 65 + 38 \log \left(\frac{21\theta - 19}{4} \right) = 0.$$

Then, for any $\theta < \theta_1$,

$$\#\{p_1, p_2, p_3 : p_i \sim x, p_i \ prime, P^+(p_1 p_2 + p_1 p_3 + p_2 p_3) > x^\theta\} \gg_\theta \frac{x^3}{(\log x)^3}.$$

Extending our methods we can give a version of Theorem 1.1 which, like Baker's bound (2), is nontrivial for $x \geqslant q^{\frac{1}{2}+\delta}$. We will only prove this result in the following qualitative form.

Theorem 1.3. *For any $\delta > 0$ there exists an $\eta > 0$ such that*

$$\sum_{q \sim Q} \max_{(a,q)=1} |S_q(a;x)| \ll_\delta Qx^{1-\eta},$$

provided that $Q \geqslant x \geqslant Q^{\frac{1}{2}+\delta}$.

In some applications of Theorem 1.1 the maximum over a is not necessary. We therefore prove a bound when a is constant, which is stronger provided that a is not too large.

Theorem 1.4. *For any integer $a > 0$ and any $\epsilon > 0$ we have*

$$\sum_{q \sim Q} |S_q(a;x)| \ll_\epsilon \left(1 + \frac{a}{xQ}\right)^{\frac{1}{2}} \left(Q^{\frac{1}{2}} x^{\frac{11}{8}} + Q^{\frac{7}{6}} x^{\frac{2}{3}}\right) (aQ)^\epsilon$$

for $Q^{\frac{4}{3}} \geqslant x \geqslant Q^{\frac{1}{2}}$.

This is nontrivial for $Q^{\frac{1}{2}+\delta} \leqslant x \leqslant Q^{\frac{4}{3}-\delta}$. The proof exploits the fact that, since there is no maximum over a, we can reorder summations to give an inner sum over $q \sim Q$. This is a longer range than those arising in the proof of Theorem 1.1. After inverting the Kloosterman fractions in such sums we reach a situation in which the Weil estimate for short Kloosterman sums can be used.

The sums in this last theorem are essentially bilinear forms with Kloosterman fractions, which were studied for arbitrary coefficients by Duke, Friedlander and Iwaniec in [3]. In the case that one of the coefficients is the indicator function of the primes then our theorem does better than the general result of [3], provided that x and Q are sufficiently close in size.

Our paper, [6], makes use of Theorem 1.4. In it we show that, for any irrational α and any $\tau < \frac{8}{23}$, there exist infinitely many n with precisely two prime factors for which the distance from $n\alpha$ to the nearest integer is at most $n^{-\tau}$. The significance of the exponent $\frac{8}{23}$ is that it is greater than the limit $\frac{1}{3}$ which an approach via GRH encounters.

We are most interested in the situation when $x \asymp Q$, that is $Q \ll x \ll Q$, as this is the case in our application to Diophantine approximation. For this reason we have given theorems which, given our current ideas, are as sharp as possible in this case. For x sufficiently different in size to Q it is possible to improve the above theorems. In order to compare the various results we note that when $x \asymp Q$ we have the following bounds, valid for any $\epsilon > 0$.

1. Using Fouvry and Shparlinski's bound (1) or Baker's (2), we get

$$\sum_{q \sim Q} \max_{(a,q)=1} |S_q(a;x)| \ll_\epsilon Q^{\frac{23}{12}+\epsilon}.$$

2. Theorem 1.1 improves this to

$$\sum_{q \sim Q} \max_{(a,q)=1} |S_q(a;x)| \ll_\epsilon Q^{\frac{19}{10}+\epsilon}.$$

3. If $0 < a \ll Q^2$ then using Theorem 2 from Duke, Friedlander and Iwaniec [3], we get a bound

$$\sum_{q \sim Q} |S_q(a;x)| \ll_\epsilon Q^{\frac{95}{48}+\epsilon}.$$

4. If $0 < a \ll Q^2$ then Theorem 1.4 gives a bound

$$\sum_{q \sim Q} |S_q(a;x)| \ll_\epsilon Q^{\frac{15}{8}+\epsilon}.$$

These bounds should be compared with the trivial bound of Q^2 and the conjectured best bound of $Q^{\frac{3}{2}+\epsilon}$.

2. Lemmas

We require the following estimate for short Kloosterman sums coming from the Weil bound.

Lemma 2.1. *For integers a and q with $q > 1$, and reals $Y < Z$ we have, for any $\epsilon > 0$, that*

$$\sum_{\substack{Y < n \leqslant Z \\ (n,q)=1}} e(\frac{a\overline{n}}{q}) \ll_\epsilon \left((a,q) \left(\frac{Z-Y}{q} + 1 \right) + q^{\frac{1}{2}} \right) q^\epsilon.$$

Proof. This is a slight weakening of Lemma 1 from Fouvry and Shparlinski, [4]. It follows immediately on inserting the estimate

$$n^{1-\epsilon} \ll \phi(n) \ll n$$

as well as the standard bound for the divisor function, τ, into that lemma.   ∎

We also require the following estimate for the number of solutions to a certain Diophantine equation.

Lemma 2.2. *Let $k \in \mathbb{N}$ and $\epsilon > 0$ be fixed. For any $N \geqslant 0$ we have*

$$\# \left\{ (n_1, \ldots, n_{2k}) \in \mathbb{Z}^{2k} : 0 < n_i \leqslant N, \sum_{i=1}^{k} \frac{1}{n_i} = \sum_{i=k+1}^{2k} \frac{1}{n_i} \right\} \ll_{\epsilon, k} N^{k+\epsilon}.$$

Proof. This is well known. For example, it follows from Karatsuba's first lemma in [7]. The key idea is that if $n_1, \ldots, n_{2k}$ is a solution then the product $n_1 \ldots n_{2k}$ must be square-full. ∎

Now let $J_M^{(k)}(q)$ denote the number of solutions to the congruence

$$\overline{m}_1 + \ldots + \overline{m}_k \equiv \overline{m}_{k+1} + \ldots + \overline{m}_{2k} \pmod{q} \tag{3}$$

with $1 \leqslant m_i \leqslant M$ and $(m_i, q) = 1$. The following generalises Fouvry and Shparlinski's result, [4, Lemma 3].

Lemma 2.3. *Fix some $k \in \mathbb{N}$. For any $\epsilon > 0$ and any $M \geqslant 1$ we have*

$$\sum_{q \sim Q} J_M^{(k)}(q) \ll_{k, \epsilon} (QM^k + M^{2k}) M^\epsilon.$$

Proof. For each $(m_1, \ldots, m_{2k})$ with $1 \leqslant m_i \leqslant M$ we count the number of $q \sim Q$ with $(q, m_i) = 1$ for which the congruence (3) holds. If

$$\frac{1}{m_1} + \ldots + \frac{1}{m_k} = \frac{1}{m_{k+1}} + \ldots + \frac{1}{m_{2k}}$$

then the congruence is satisfied for every $q \sim Q$ for which q is coprime to $\prod m_i$. Using Lemma 2.2 it follows that the contribution from such $2k$-tuples $(m_1, \ldots, m_{2k})$ is

$$O_{\epsilon, k}(QM^{k+\epsilon}).$$

In the alternative case we define

$$F = \prod_{i=1}^{2k} m_i \left(\sum_{i=1}^{k} m_i^{-1} - \sum_{i=k+1}^{2k} m_i^{-1} \right)$$

so that F is a non-zero integer with $|F| \ll M^{2k}$. Since $q | F$ there are $O(M^\epsilon)$ possible values for q. Thus the contribution from such $2k$-tuples $(m_1, \ldots, m_{2k})$ is

$$O_{\epsilon, k}(M^{2k+\epsilon})$$

so the result follows. ∎

3. Estimates for Bilinear Sums

Throughout this section let α_l, β_m be arbitrary complex numbers bounded by 1. We will prove estimates for sums

$$W_{a,q} = \sum_{\substack{l \sim L, m \sim M \\ (ml,q)=1}} \alpha_l \beta_m e\left(\frac{a\overline{lm}}{q}\right),$$

either individually or on average over $q \sim Q$. If $\beta_m = 1$ then we call $W_{a,q}$ a Type I sum, if not then it is Type II.

Firstly we use Lemma 2.3 to estimate Type II sums on average. This is a generalisation of a bound of Fouvry and Shparlinski, [4, Corollary 5].

Lemma 3.1. *Suppose that* $1 \leqslant L, M \leqslant Q$. *For any integer* $k \geqslant 1$ *and any* $\epsilon > 0$ *we have*

$$\sum_{q \sim Q} \max_{(a,q)=1} |W_{a,q}| \ll_{\epsilon,k} Q\left(Q^{\frac{1}{2k}} L^{\frac{2k-1}{2k}} M^{\frac{1}{2}} + L^{\frac{2k-1}{2k}} M\right) Q^{\epsilon}.$$

Proof. By Hölder's inequality we have

$$|W_{a,q}|^{2k} \leqslant L^{2k-1} \sum_{\substack{l \sim L \\ (l,q)=1}} \left| \sum_{\substack{m \sim M \\ (m,q)=1}} \beta_m e\left(\frac{a\overline{lm}}{q}\right) \right|^{2k}.$$

Since $L < Q$ we may bound this by extending the sum over l to a sum over all residues modulo q:

$$|W_{a,q}|^{2k} \leqslant L^{2k-1} \sum_{l=1}^{q} \left| \sum_{\substack{m \sim M \\ (m,q)=1}} \beta_m e\left(\frac{al\overline{m}}{q}\right) \right|^{2k}.$$

Expanding, reordering the summation and using the orthogonality of additive characters then results in

$$|W_{a,q}|^{2k} \ll L^{2k-1} Q J_M^{(k)}(q).$$

Using Hölder's inequality and Lemma 2.3 we then get

$$\sum_{q \sim Q} \max_{(a,q)=1} |W_{a,q}| \ll L^{\frac{2k-1}{2k}} Q^{\frac{1}{2k}} \sum_{q \sim Q} J_M^{(k)}(q)^{\frac{1}{2k}}$$

$$\leqslant L^{\frac{2k-1}{2k}} Q \left(\sum_{q \sim Q} J_M^{(k)}(q) \right)^{\frac{1}{2k}}$$

$$\ll_{\epsilon,k} L^{\frac{2k-1}{2k}} Q (QM^k + M^{2k})^{\frac{1}{2k}} M^{\epsilon}$$

$$\ll Q(Q^{\frac{1}{2k}} L^{\frac{2k-1}{2k}} M^{\frac{1}{2}} + L^{\frac{2k-1}{2k}} M) Q^{\epsilon}. \qquad \blacksquare$$

If we remove the maximum over a then we can obtain a sharper estimate by exploiting the sum over q.

Lemma 3.2. *For any integer $a > 0$, any $L, M, Q \geqslant 1$, and any $\epsilon > 0$, we have*

$$\sum_{q \sim Q} |W_{a,q}| \ll_\epsilon \left(1 + \frac{a}{LMQ} \right)^{\frac{1}{2}} \left(QLM^{\frac{1}{2}} + Q^{\frac{1}{2}} L^{\frac{5}{4}} M^{\frac{3}{2}} \right) (aQ)^\epsilon.$$

Proof. We first consider the case when α_l, β_m are supported on integers coprime to a. We trivially have

$$\sum_{q \sim Q} |W_{a,q}| \leqslant \sum_{\substack{l \sim L \\ (l,a)=1}} W_1(l)$$

where

$$W_1(l) = \sum_{\substack{q \sim Q \\ (q,l)=1}} \left| \sum_{\substack{m \sim M \\ (m,aq)=1}} \beta_m e \left(\frac{a\overline{lm}}{q} \right) \right|.$$

By Cauchy's inequality we get

$$W_1(l)^2 \leqslant Q \sum_{\substack{q \sim Q \\ (q,l)=1}} \left| \sum_{\substack{m \sim M \\ (m,aq)=1}} \beta_m e \left(\frac{a\overline{lm}}{q} \right) \right|^2.$$

Expanding and reordering the summation then gives us the bound

$$W_1(l)^2 \leqslant Q \sum_{\substack{m_1, m_2 \sim M \\ (m_1 m_2, a)=1}} \left| \sum_{\substack{q \sim Q \\ (q, lm_1 m_2)=1}} e \left(\frac{a(m_1 - m_2)\overline{lm_1 m_2}}{q} \right) \right|.$$

We can write

$$\overline{lm_1 m_2} = \frac{1 - q\overline{q}}{lm_1 m_2}$$

where $\overline{q}$ is an inverse of q modulo $lm_1 m_2$. Therefore

$$W_1(l)^2 \leqslant Q \sum_{\substack{m_1, m_2 \sim M \\ (m_1 m_2, a)=1}} \left| \sum_{\substack{q \sim Q \\ (q, lm_1 m_2)=1}} e \left(\frac{a(m_1 - m_2)}{qlm_1 m_2} \right) e \left(-\frac{a(m_1 - m_2)\overline{q}}{lm_1 m_2} \right) \right|.$$

If we let

$$f(t) = e \left(\frac{a(m_1 - m_2)}{lm_1 m_2 t} \right)$$

then the factor $f(q)$ can be removed using summation by parts. For $t \sim Q$ we have

$$f'(t) \ll \frac{a}{LMQ^2}$$

and thus

$$W_1(l)^2 \ll Q\left(1 + \frac{a}{LMQ}\right) \sum_{\substack{m_1,m_2 \sim M \\ (m_1 m_2, a)=1}} \max_{Q' \sim Q} \left| \sum_{\substack{Q \leqslant q < Q' \\ (q, lm_1 m_2)=1}} e\left(\frac{a(m_1 - m_2)\overline{q}}{lm_1 m_2}\right) \right|.$$

We get a contribution to this from pairs $m_1 = m_2$ which is bounded by

$$Q\left(1 + \frac{a}{LMQ}\right)MQ.$$

For the remaining terms let

$$b = a(m_1 - m_2)$$

and

$$c = lm_1 m_2$$

so that the inner sum is

$$\sum_{\substack{Q \leqslant q < Q' \\ (q,c)=1}} e\left(\frac{b\overline{q}}{c}\right).$$

We may bound this using Lemma 2.1 by

$$O_\epsilon\left(((b,c)\left(\frac{Q}{LM^2} + 1\right) + (LM^2)^{\frac{1}{2}})(LM^2)^\epsilon\right).$$

The result would be trivial if $LM^2 \geqslant Q^2$. We thus assume that $LM^2 \leqslant Q^2$, which allows us to replace $(LM^2)^\epsilon$ by Q^ϵ in our bound.

The contribution to our estimate for $W_1(l)^2$ from the term $(LM^2)^{\frac{1}{2}}$ is then

$$O_\epsilon\left(Q\left(1 + \frac{a}{LMQ}\right)L^{\frac{1}{2}}M^3 Q^\epsilon\right)$$

and that from the remaining terms is

$$O_\epsilon\left(Q\left(1 + \frac{a}{LMQ}\right)\left(\frac{Q}{LM^2} + 1\right)Q^\epsilon \sum_{\substack{m_1,m_2 \sim M \\ m_1 \neq m_2}} (m_1 - m_2, lm_1 m_2)\right),$$

where we have used that $(m_1 m_2 l, a) = 1$.

If we write $h = m_1 - m_2 \neq 0$ then

$$\sum_{\substack{m_1, m_2 \sim M \\ m_1 \neq m_2}} (m_1 - m_2, l m_1 m_2) \ll \sum_{m_1 \sim M} \sum_{0 < h \ll M} (h, l m_1(m_1 + h))$$

$$= \sum_{m_1 \sim M} \sum_{0 < h \ll M} (h, l m_1^2)$$

$$\ll_\epsilon M^2 Q^\epsilon,$$

since one has in general that

$$\sum_{h=1}^{H} (h, n) = \sum_{d|n} d \# \{h \leqslant H/d : (h, n) = 1\} \leqslant \sum_{d|n} H = H \tau(n) \ll_\epsilon H n^\epsilon$$

for any $n \in \mathbb{N}$.

We conclude that

$$W_1(l)^2 \ll_\epsilon Q \Big(1 + \frac{a}{LMQ}\Big) \Big(QM + L^{\frac{1}{2}} M^3 + \frac{Q}{L} + M^2\Big) Q^\epsilon.$$

Since $L, M \geqslant 1$ this simplifies to

$$W_1(l)^2 \ll_\epsilon Q \Big(1 + \frac{a}{LMQ}\Big) \Big(QM + L^{\frac{1}{2}} M^3\Big) Q^\epsilon$$

and therefore

$$\sum_{q \sim Q} |W_{a,q}| \ll_\epsilon \Big(1 + \frac{a}{LMQ}\Big)^{\frac{1}{2}} \Big(QLM^{\frac{1}{2}} + Q^{\frac{1}{2}} L^{\frac{5}{4}} M^{\frac{3}{2}}\Big) Q^\epsilon.$$

This completes the proof under the assumption that the coefficients are supported on integers coprime to a. To remove this assumption we begin by writing $(l, a) = u$, $a = bu$ and $l = ku$ to get

$$W_{a,q} = \sum_{\substack{l \sim L, m \sim M \\ (ml, q) = 1}} \alpha_l \beta_m e\left(\frac{a \overline{lm}}{q}\right)$$

$$= \sum_{\substack{a = ub \\ (u, q) = 1}} \sum_{\substack{k \sim L/u, m \sim M \\ (mk, q) = 1, (k, b) = 1}} \alpha_{uk} \beta_m e\left(\frac{b \overline{km}}{q}\right).$$

Next we set $(m, b) = v$, $m = vj$ and $b = cv$ to rewrite this as

$$\sum_{\substack{a = uvc \\ (uv, q) = 1}} \sum_{\substack{k \sim L/u, j \sim M/v \\ (jk, q) = 1, (k, vc) = 1, (j, c) = 1}} \alpha_{uk} \beta_{vj} e\left(\frac{c \overline{kj}}{q}\right).$$

It follows that

$$\sum_{q\sim Q} |W_{a,q}| \leqslant \sum_{\substack{a=uvc}} \sum_{\substack{q\sim Q \\ (uv,q)=1}} \left| \sum_{\substack{k\sim L/u, j\sim M/v \\ (jk,q)=1,(k,vc)=1,(j,c)=1}} \alpha_{uk}\beta_{vj} e\left(\frac{c\overline{kj}}{q}\right) \right|$$

$$\leqslant \sum_{a=uvc} \sum_{q\sim Q} \left| \sum_{\substack{k\sim L/u, j\sim M/v \\ (jk,q)=1,(k,vc)=1,(j,c)=1}} \alpha_{uk}\beta_{vj} e\left(\frac{c\overline{kj}}{q}\right) \right|.$$

For each factorisation $a = uvc$ the inner sum now has coefficients supported on integers coprime to c so the above bound applies. The number of factorisations is $O(a^\epsilon)$ so the bound for the general sum is the same as that for the sum with coprimality conditions except for an additional factor a^ϵ. ∎

Finally we use Lemma 2.1 directly, to estimate Type I sums when L is small.

Lemma 3.3. *Suppose that $\beta_m = 1$. Then, for any $L, M \geqslant 1$ and any $\epsilon > 0$ we have*

$$W_{a,q} \ll_\epsilon \left((a,q)\left(\frac{LM}{Q} + L\right) + Q^{\frac{1}{2}}L \right) Q^\epsilon.$$

Proof. We have

$$|W_{a,q}| \leqslant \sum_{\substack{l\sim L \\ (l,q)=1}} \left| \sum_{\substack{m\sim M \\ (m,q)=1}} e\left(\frac{a\overline{lm}}{q}\right) \right|.$$

The result follows on applying Lemma 2.1 to the inner sum. ∎

Summing this result over $q \sim Q$ we immediately get the following.

Lemma 3.4. *Suppose that $L, M, Q \geqslant 1$ and that $\beta_m = 1$. For any $\epsilon > 0$ we have*

$$\sum_{q\sim Q} \max_{(a,q)=1} |W_{a,q}| \ll_\epsilon (LM + Q^{\frac{3}{2}}L)Q^\epsilon.$$

In addition if $a > 0$ then we have

$$\sum_{q\sim Q} |W_{a,q}| \ll_\epsilon (LM + Q^{\frac{3}{2}}L)(aQ)^\epsilon.$$

4. Proof of the Theorems

4.1. Approach

In the sums $S_q(a; x)$ we replace the indicator function of the primes with the von Mangoldt function $\Lambda(n)$. The contribution of prime powers p^α with $\alpha > 1$ is $O_\epsilon(x^{\frac{1}{2}+\epsilon})$. This is smaller than any of the bounds we will establish so it may be ignored. In addition the factor $\log p$ may be removed using partial summation with the cost of a factor $x^\epsilon \ll Q^\epsilon$. It is thus sufficient to establish the theorems for the sums containing Λ.

We decompose $\Lambda(n)$ using Vaughan's Identity, as described by Davenport in [2, Chapter 24]. We will use $U = V \leqslant x^{\frac{1}{3}}$; the precise choice of U for each theorem will be given later. The sum $S_q(a; x)$ is decomposed into Type I and II sums with $LM \asymp x$. The precise forms of the sums are given by Fouvry and Shparlinski in [4]. The coefficients are not all bounded by 1 but they are bounded by a divisor function. This divisor function may be absorbed into the Q^ϵ term. We must estimate Type I sums for $L \leqslant U^2$ and Type II sums for $U \leqslant L \leqslant x/U$. Since $U^2 \leqslant x/U$ any Type I sum with $U \leqslant L \leqslant U^2$ may be regarded as a Type II sum. Hence it will be enough to consider Type I sums with $L \leqslant U$ and Type II sums with $U \leqslant L \leqslant x/U$. The variables of summation are restricted by the condition $lm \sim x$. In the Type II sums this may be removed by Fourier analysis, see for example the start of Garaev's proof, [5, Lemma 2.4]. For the Type I sums, if we are simply treating them as Type II sums then the same argument applies, whereas if we are using Lemma 3.4 then it is clear that a condition $lm \sim x$ can be introduced by modifying the proof.

4.2. Proof of Theorem 1.1

The sums arising from Vaughan's identity are of the form

$$\sum_{q \sim Q} \max_{(a,q)=1} |W_{a,q}|.$$

We estimate the Type II sums using Lemma 3.1. We have

$$L, M \leqslant \frac{x}{U}$$

and thus the hypotheses are satisfied provided that our choice of U satisfies $\frac{x}{U} \leqslant Q$. Recalling that $M \ll x/L$ the bound from Lemma 3.1 is

$$Q\Big(Q^{\frac{1}{2k}} x^{\frac{1}{2}} L^{\frac{k-1}{2k}} + xL^{\frac{-1}{2k}}\Big)Q^\epsilon.$$

For $x^{\frac{2}{5}} \leqslant L \leqslant x^{\frac{1}{2}}$ we apply this with $k = 2$ to get a bound of

$$Q\Big(Q^{\frac{1}{4}} x^{\frac{5}{8}} + x^{\frac{9}{10}}\Big)Q^\epsilon.$$

For $x^{\frac{3}{5}} \leqslant L \leqslant x/U$ we use $k = 3$ to get

$$Q\Big(Q^{\frac{1}{6}}x^{\frac{5}{6}}U^{-\frac{1}{3}} + x^{\frac{9}{10}}\Big)Q^{\epsilon}.$$

Since $LM \asymp x$ and we can interchange l, m in our sums these two bounds in fact cover the whole range $U \leqslant L \leqslant x/U$. The contribution of all our Type II sums is therefore

$$O_{\epsilon}\left(Q\Big(Q^{\frac{1}{4}}x^{\frac{5}{8}} + x^{\frac{9}{10}} + Q^{\frac{1}{6}}x^{\frac{5}{6}}U^{-\frac{1}{3}}\Big)Q^{\epsilon}\right).$$

We need to estimate Type I sums for $L \leqslant U$. Lemma 3.4 gives a bound for these sums of

$$\Big(x + Q^{\frac{3}{2}}U\Big)Q^{\epsilon}.$$

Since $x \leqslant Q^{\frac{3}{2}}$ and $U \geqslant 1$ the second term is larger and thus

$$\sum_{q \sim Q} \max_{(a,q)=1} |S_q(a;x)| \ll_{\epsilon} Q\Big(Q^{\frac{1}{4}}x^{\frac{5}{8}} + x^{\frac{9}{10}} + Q^{\frac{1}{6}}x^{\frac{5}{6}}U^{-\frac{1}{3}} + Q^{\frac{1}{2}}U\Big)Q^{\epsilon}.$$

We now choose

$$U = \min\Big(x^{\frac{1}{3}}, Q^{-\frac{1}{4}}x^{\frac{5}{8}}\Big).$$

Since $Q^{\frac{2}{3}} \leqslant x \leqslant Q^{\frac{3}{2}}$ we have

$$1 \leqslant U \leqslant x^{\frac{1}{3}}$$

and

$$\frac{x}{U} \leqslant Q.$$

This choice of U is therefore admissible so we can conclude that

$$\sum_{q \sim Q} \max_{(a,q)=1} |S_q(a;x)| \ll_{\epsilon} Q\Big(Q^{\frac{1}{4}}x^{\frac{5}{8}} + x^{\frac{9}{10}} + Q^{\frac{1}{6}}x^{\frac{13}{18}}\Big)Q^{\epsilon},$$

thus proving Theorem 1.1.

4.3. Proof of Theorem 1.2

The following lemma generalises Baker's analysis, [1, Section 4].

Lemma 4.1. *Let $\beta > 0$ be fixed. Suppose $\alpha \in (1,2)$ is a constant such that for any $\epsilon > 0$ there exists a $\delta > 0$ for which*

$$\sum_{q \sim Q} \max_{(a,q)=1} \left| \sum_{\substack{x \leqslant p < (1+\beta)x \\ (p,q)=1}} e\left(\frac{a\overline{p}}{q}\right) \right| \ll_{\beta,\epsilon} x^{2-\delta} \tag{4}$$

holds for $x \leqslant Q \leqslant x^{\alpha-\epsilon}$. We may then deduce Theorem 1.2 with θ_1 the root of the equation

$$2\theta - \alpha - 2 + 2(2-\alpha)\log\left(\frac{\theta + \alpha - 2}{2\alpha - 2}\right) = 0.$$

Proof. Using our hypothesis (4) in the proof of [1, Theorem 4] we see that it holds with the exponent $\frac{13}{12}$ replaced by our constant α. We now use an almost identical proof to that of [1, Theorem 3]. We replace $Y := x^{13/12-\epsilon}$ by $Y := x^{\alpha-\epsilon}$. The asymptotic [1, (4.11)] becomes

$$\sum_1 \sim (\alpha - \epsilon)X\mathcal{L}.$$

Baker's quantity J is now given by

$$J = \frac{\log(Z/Y)}{\mathcal{L}} + \frac{\log(x^2/Y)}{\mathcal{L}} \log\left[\frac{\log(YZx^{-2})}{\log(Y^2x^{-2})}\right]$$

$$= \theta - \alpha + \epsilon + (2 - \alpha + \epsilon)\log\left[\frac{\theta + \alpha - \epsilon - 2}{2\alpha - 2\epsilon - 2}\right].$$

The bound [1, (4.21)] now becomes

$$\sum_3 \leqslant (2 + 2\epsilon)\pi(x, \beta)^3\left(1 + \frac{2\log(1+\beta)}{\log 2}\right)$$

$$\times \left[\theta - \alpha + \epsilon + (2 - \alpha + \epsilon)\log\frac{\theta + \alpha - \epsilon - 2}{2\alpha - 2\epsilon - 2}\right].$$

Since $\theta < \theta_1$ we may choose ϵ, β sufficiently small to get a bound of

$$\sum_3 < (2 - \alpha - \epsilon)\pi(x, \beta)^3\mathcal{L}.$$

The result follows. ∎

Theorem 1.1 shows that the hypotheses of this lemma are satisfied with $\alpha = \frac{23}{21}$. We only gave the proof for $\beta = 1$ but it is clear that it can be modified to handle any fixed β. The equation defining θ_1 is thus

$$42\theta - 65 + 38\log\left(\frac{21\theta - 19}{4}\right) = 0.$$

The root of this is $\theta = 1.188\ldots$, as given in Theorem 1.2.

4.4. Proof of Theorem 1.3

For $\delta > \frac{1}{6}$ the result follows from Theorem 1.1 so we assume that $\delta \leqslant \frac{1}{6}$. Since we do not require the result to be optimal we take

$$U = Q^{\frac{\delta}{2}}.$$

It is then sufficient to estimate Type II sums for

$$x^{\frac{1}{2}} \leqslant L \leqslant xQ^{-\frac{\delta}{2}}.$$

Since $x \leqslant Q$ we know that $L, M \leqslant Q$ so the hypotheses for Lemma 3.1 are satisfied and we get a bound

$$Q\left(Q^{\frac{2-\delta(k-1)}{4k}} x^{\frac{2k-1}{2k}} + x^{1-\frac{1}{4k}}\right)Q^{\epsilon}.$$

We may choose $k = k_0$ sufficiently large in terms of δ so that

$$2 - \delta(k_0 - 1) < 0.$$

Our Type II sum is therefore bounded by

$$Q\left(x^{1-\frac{1}{2k_0}} + x^{1-\frac{1}{4k_0}}\right)Q^{\epsilon} \ll Q^{1+\epsilon}x^{1-\frac{1}{4k_0}}.$$

We also require an estimate for a Type I sum with $L \leqslant Q^{\frac{\delta}{2}}$. From Lemma 3.4 such sums may be bounded by

$$\left(x + Q^{\frac{3+\delta}{2}}\right)Q^{\epsilon}.$$

Since $x \leqslant Q$ the second term in this estimate is larger. Furthermore $x \geqslant Q^{\frac{1}{2}+\delta}$ so

$$Q^{\frac{1+\delta}{2}} \leqslant x^{\frac{1+\delta}{1+2\delta}}.$$

We conclude that

$$\sum_{q \sim Q} \max_{(a,q)=1} |S_q(a;x)| \ll_{\delta,\epsilon} Q\left(x^{1-\frac{1}{4k_0}} + x^{\frac{1+\delta}{1+2\delta}}\right)Q^{\epsilon}.$$

Since this holds for any $\epsilon > 0$ the result follows on taking

$$\eta < \min\left(\frac{1}{4k_0}, \frac{\delta}{1+2\delta}\right).$$

4.5. Proof of Theorem 1.4

The sums arising from Vaughan's identity are now of the form

$$\sum_{q \sim Q} |W_{a,q}|.$$

We estimate the Type II sums using Lemma 3.2. Since $LM \asymp x$ this gives a bound

$$\left(1 + \frac{a}{xQ}\right)^{\frac{1}{2}}\left(Qx^{\frac{1}{2}}L^{\frac{1}{2}} + Q^{\frac{1}{2}}x^{\frac{3}{2}}L^{-\frac{1}{4}}\right)(aQ)^{\epsilon}.$$

It is sufficient to estimate the Type II sums for $x^{\frac{1}{2}} \leqslant L \leqslant x/U$. In this range we get a bound of

$$\left(1 + \frac{a}{xQ}\right)^{\frac{1}{2}}\left(QxU^{-\frac{1}{2}} + Q^{\frac{1}{2}}x^{\frac{11}{8}}\right)(aQ)^{\epsilon}.$$

Lemma 3.4 gives us a bound for the Type I sums with $L \leqslant U$ of $Q^{\frac{3}{2}+\epsilon}Ua^{\epsilon}$. We now choose
$$U = \min\left(x^{\frac{1}{3}}, Q^{-\frac{1}{3}}x^{\frac{2}{3}}\right).$$

Since $x \geqslant Q^{\frac{1}{2}}$ we have
$$1 \leqslant U \leqslant x^{\frac{1}{3}}.$$

This choice of U is therefore admissible and we get

$$\sum_{q \sim Q} |S_q(a;x)| \ll_{\epsilon} \left(1 + \frac{a}{xQ}\right)^{\frac{1}{2}}\left(Qx^{\frac{5}{6}} + Q^{\frac{7}{6}}x^{\frac{2}{3}} + Q^{\frac{1}{2}}x^{\frac{11}{8}}\right)(aQ)^{\epsilon}.$$

If $x \leqslant Q$ then
$$Qx^{\frac{5}{6}} \leqslant Q^{\frac{7}{6}}x^{\frac{2}{3}}$$

and if $x \geqslant Q$ then
$$Qx^{\frac{5}{6}} \leqslant Q^{\frac{1}{2}}x^{\frac{11}{8}}.$$

The term $Qx^{\frac{5}{6}}$ is therefore not necessary in our bound so Theorem 1.4 follows.

References

[1] R.C. Baker, *Kloosterman sums with prime variable*, Acta Arith. **156**(3) (2012), 351–372.

[2] H. Davenport, *Multiplicative number theory*, volume 74 of Graduate Texts in Mathematics, Springer-Verlag, New York, second edition, 1980, revised by Hugh L. Montgomery.

[3] W. Duke, J. Friedlander, and H. Iwaniec, *Bilinear forms with Kloosterman fractions*, Invent. Math. **128**(1) (1997), 23–43.

[4] É. Fouvry and I.E. Shparlinski, *On a ternary quadratic form over primes*, Acta Arith. **150**(3) (2011), 285–314.

[5] M.Z. Garaev, *An estimate for Kloosterman sums with primes and its application*, Mat. Zametki **88**(3) (2010), 365–373.

[6] A.J. Irving, *Diophantine approximation with products of two primes*, J. Lond. Math. Soc. (2) **89** (2014), no. 2, 581–602.

[7] A.A. Karatsuba, *Analogues of Kloosterman sums*, Izv. Ross. Akad. Nauk Ser. Mat. **59**(5) (1995), 93–102.

Address: Alastair J. Irving: Mathematical Institute, 24–29, St. Giles', Oxford OX1 3LB, UK.

E-mail: irving@maths.ox.ac.uk