EFFECTIVE MOMENTS OF DIRICHLET $L$-FUNCTIONS IN GALOIS ORBITS

RIZWANUR KHAN, RUOYUN LEI, AND DJORDJE MILIČEVIĆ

Abstract. Khan, Miličević, and Ngo evaluated the second moment of $L$-functions associated to certain Galois orbits of primitive Dirichlet characters to modulus a large power of any fixed odd prime $p$. Their results depend on $p$-adic Diophantine approximation and are ineffective, in the sense of computability. We obtain an effective asymptotic for this second moment in the case of $p = 3, 5, 7$.

1. Introduction

Dirichlet $L$-functions, introduced by Dirichlet in 1837, are the first generalization of the Riemann zeta function. They are extremely important in number theory, being used for example to study the number of primes in arithmetic progressions and the class number of certain number fields (via Dirichlet’s class number formula). Given a primitive Dirichlet character $\chi$ with modulus $q$ (see [5] for further background), the associated $L$-function is defined for $\Re(s) > 1$ by the absolutely convergent series

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}. \quad (1.1)$$

This has an Euler product

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

and analytically continues to an entire function with functional equation

$$\Lambda(s, \chi) := \left(\frac{\pi}{q}\right)^{-\nu_s/2} \Gamma\left(\frac{s + \kappa}{2}\right) L(s, \chi) = \frac{\tau(\chi)}{i^\nu q^{1/2}} \Lambda(1 - s, \overline{\chi}),$$

where $\tau(\chi)$ is the Gauss sum and

$$\kappa := \begin{cases} 0 & \text{if } \chi(-1) = 1, \\ 1 & \text{if } \chi(-1) = -1. \end{cases} \quad (1.2)$$

As is typically the case, the line of symmetry $\Re(s) = \frac{1}{2}$ of the functional equation is where the $L$-function is most difficult to understand. Since the values at $s = \frac{1}{2}$ of $L$-function often encode important arithmetic information, it is natural to consider the central values $L(\frac{1}{2}, \chi)$. From the adelic point of view, these may be considered as finite-place-twist analogs of the archimedean twist $\zeta(\frac{1}{2} + it)$, which is of classical interest in analytic number theory. For example, it is conjectured that the central value $L(\frac{1}{2}, \chi)$ is never zero, but only partial results exist in this direction [1, 10, 16]. As another example, an analogue of the Lindelöf conjecture asserts that $L(\frac{1}{2}, \chi) \ll q^\epsilon$ for any $\epsilon > 0$, but again only partial results exist [2, 4, 11]. (Here and henceforth, $\epsilon$ will always be used to denote an arbitrarily small positive constant, but may not be the same from one occurrence to the next. All implicit constants may depend on $\epsilon$.)

Given the lack of “closed-form formulas” that would directly shed light on the values of individual $L(\frac{1}{2}, \chi)$, one often thinks of $L$-functions as embedded in families and of the central value $L(\frac{1}{2}, \chi)$. 

2010 Mathematics Subject Classification. 11M20.

Key words and phrases. $L$-functions, Dirichlet characters, moments.
as a random variable whose distribution we are trying to understand. From probability theory, we
know that one way to understand the distribution of a random variable is to find its moments. For
example, given a large sample of test scores, the first moment tells us the average score, the second
moment is related to the variance of the scores, and if, as is often the case for test scores, their
distribution follows the bell curve, then the \( n \)-th moment of the observed scores should correspond
to that of the (rescaled) normal distribution. This philosophy about computing moments is in fact
a typical starting point in solving problems about nonvanishing and size in families of \( L \)-functions.

We remark on the side that numerics, partial theoretical results including the known moments, as
well as analogs over function fields support a general conjecture that families of \( L \)-functions exhibit
random behavior in a suitable sense (see, for example, [8]).

The moments problem is to evaluate asymptotically (as \( q \to \infty \))

\[
\sum_{\chi \mod q}^* L(\frac{1}{2}, \chi)^n
\]

for all \( n \in \mathbb{N} \), as well as

\[
\sum_{\chi \mod q}^* |L(\frac{1}{2}, \chi)|^n
\]

for even values of \( n \), where \( \sum^* \) means that the summation is restricted to the primitive characters.
The evaluation of the first and second moments (\( n = 1, 2 \)) is classical and due to Paley [12]. The
third and fourth moments (\( n = 3, 4 \)) are quite recent and due to Zacharias [19] and Young [18]
respectively. Nothing is known for \( n \geq 5 \).

In this paper we are interested in moments over natural subsets of the primitive Dirichlet char-
ters \( \mod q \), where \( q \) is of a special form. Working over a smaller set gets us closer to the true
asymptotic features of individual \( L \)-functions, but of course it also means that there are fewer ‘har-
monics’ available to average over, so the evaluation of the moments becomes more difficult. We now
proceed to describe our set of characters.

Let \( \xi \) be a primitive \( \phi(q) \)-th root of unity, where \( \phi \) is the Euler totient function, and let \( \mathbb{Q}(\xi) \)
be the corresponding cyclotomic field, which is Galois over \( \mathbb{Q} \). The group \( G = \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \) acts
on the set of primitive Dirichlet characters modulo \( q \) as follows. For \( \sigma \in G \), we define \( \chi^\sigma \) to be
that character for which \( \chi^\sigma(n) = \sigma(\chi(n)) \) for all \( (n, q) = 1 \). The action under \( G \) partitions the
set of characters into orbits \( \mathcal{O} \), which we usually refer to as Galois orbits. Thus, from an algebraic
perspective, any two characters in a single orbit \( \mathcal{O} \) are indistinguishable.

<table>
<thead>
<tr>
<th>( n \mod 9 )</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>5</th>
<th>7</th>
<th>8</th>
<th>primitive?</th>
<th>order</th>
<th>in orbit:</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi_0(n) )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>yes</td>
<td>1</td>
<td>( {\chi_0} )</td>
</tr>
<tr>
<td>( \chi_1(n) )</td>
<td>1</td>
<td>( \xi )</td>
<td>( \xi^2 )</td>
<td>( \xi^5 )</td>
<td>( \xi^4 )</td>
<td>-1</td>
<td>yes</td>
<td>3 \cdot 2</td>
<td>( {\chi_1, \chi_2} )</td>
</tr>
<tr>
<td>( \chi_2(n) )</td>
<td>1</td>
<td>( \xi^2 )</td>
<td>( \xi^4 )</td>
<td>( \xi^4 )</td>
<td>( \xi^2 )</td>
<td>1</td>
<td>yes</td>
<td>3 \cdot 1</td>
<td>( {\chi_2, \chi_4} )</td>
</tr>
<tr>
<td>( \chi_3(n) )</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>no</td>
<td>2</td>
<td>( {\chi_3} )</td>
</tr>
<tr>
<td>( \chi_4(n) )</td>
<td>1</td>
<td>( \xi^4 )</td>
<td>( \xi^2 )</td>
<td>( \xi^2 )</td>
<td>( \xi^4 )</td>
<td>1</td>
<td>yes</td>
<td>3 \cdot 1</td>
<td>( {\chi_2, \chi_4} )</td>
</tr>
<tr>
<td>( \chi_5(n) )</td>
<td>1</td>
<td>( \xi^5 )</td>
<td>( \xi^4 )</td>
<td>( \xi )</td>
<td>( \xi^2 )</td>
<td>-1</td>
<td>yes</td>
<td>3 \cdot 2</td>
<td>( {\chi_1, \chi_5} )</td>
</tr>
</tbody>
</table>

Table 1. Four of the six characters modulo 9 = 3\(^2\) are primitive; they fall into two
orbits corresponding to \( d = 1 \) and \( d = 2 \).

Several works have studied the average values of \( L \)-functions over these orbits [3, 6, 9, 14]. For
the rest of the paper, we specialize to moduli of the form

\[
q = p^k,
\]

where \( p \) is a fixed odd prime (thus \( q \to \infty \) is equivalent to \( k \to \infty \)). For such moduli, the orbits
under the action of \( G \) are easy to describe. We have that \( \chi_1 \) and \( \chi_2 \) belong to the same orbit if and
only if $\chi_1$ and $\chi_2$ have the same order in the group of characters mod $q$. The possible orders are $l = p^{k-1}d$, for $d|(p-1)$, and the primitive characters of order $l$ form an orbit $O$ of cardinality $\phi(l)$. These facts are justified in [9].

In the course of studying nonvanishing of Dirichlet $L$-functions within the Galois orbits described above, Ngo and the first and third authors proved in [9, Theorem 1.2b] the following asymptotic for the second moment (as $k \to \infty$): for any given orbit $O$ and $\epsilon > 0$, we have

\begin{equation}
\frac{1}{|O|} \sum_{\chi \in O} |L(\frac{1}{2}, \chi)|^2 = \frac{p-1}{p} \log q + O(q^{-1/4+\epsilon}),
\end{equation}

where

\[ C = \frac{\Gamma'(\frac{1+2\epsilon}{2})}{\Gamma(\frac{1+2\epsilon}{2})} + 2\gamma + 2\frac{\log p}{p-1} - \log \pi, \]

log is the natural logarithm, $\gamma = 0.57721\cdots$ is the Euler constant, and $\kappa$ is defined in (1.2).

The implicit constant in the error term of (1.3) is ineffective. This means that the error term is $\leq C'q^{-1/4+\epsilon}$ for some constant $C' = C'(p, \epsilon)$, but we have no way of computing $C'$ given the values of $p$ and $\epsilon$. In turn, this means that there is a constant $k_0$ such that for all $k > k_0$, the main term of (1.3) dominates the error term, but there is no way to give an explicit value for $k_0$. In other words, we do not know how large $k$ must be before the given main term is a useful estimate of the second moment. This ineffectivity is a side effect of the fact that the argument for (1.3) given in [9] hinges crucially on Roth’s theorem in Diophantine approximation (more precisely, on the $p$-adic version of Roth’s theorem due to Ridout [13]), which is well known to be ineffective. The goal of this paper is to remedy this situation for natural towers of characters to powers of several primes $p$.

**Theorem 1.1.** Let $p = 3, 5$ or 7. For every $q = p^k$ $(k \geq 1)$ and every Galois orbit $O$ of characters modulo $q$, we have that

\[ \frac{1}{|O|} \sum_{\chi \in O} |L(\frac{1}{2}, \chi)|^2 = \frac{p-1}{p} \log q + O(q^{-\lambda_3+\epsilon}), \]

where $\lambda_3 = 1/2$ and $\lambda_5 = \lambda_7 = 1/6$. The implicit constant is computable.

Our argument differs from that of [9] in that we do not appeal to Roth’s theorem. Given the power saving error term, it should be possible to extend our main theorem to include a mollifier. This would give an effective version of the nonvanishing result given in [9, Theorem 1.2b], but only for $p = 3, 5, 7$ and with possibly smaller proportions of nonvanishing.

In the statement of Theorem 1.1 and for the rest of the paper, the asymptotic notations $f \ll g$ and $f = O(g)$ mean that $|f| \leq Cg$ for some constant $C > 0$, which may depend on $\epsilon > 0$, but is always computable for any given value of $\epsilon$.

This article grew out of Lei’s thesis at Bryn Mawr College, jointly supervised by Khan and Milićević. Milićević was supported by the National Science Foundation, Grant DMS-1503629.

**2. Preliminaries**

We first state a result which follows directly from [9, Lemma 2.3]. This illustrates an orthogonality property within orbits.

**Lemma 2.1.** Suppose $q = p^k$ for an odd prime $p$ and $k \geq 1$, $O$ is a Galois orbit of primitive Dirichlet characters mod $q$, and $n$ and $m$ are integers coprime to $p$. Clearly, $\frac{1}{|O|} |\sum_{\chi \in O} \chi(n)\chi(m)| \leq 1$. But if

\[ n^{p-1} \not\equiv m^{p-1} \mod p^{k-1}, \]

then

\[ \frac{1}{|O|} \sum_{\chi \in O} \chi(n)\chi(m) = 0. \]
Next we state a standard result from analytic number theory, called the approximate functional equation. The approximate functional equation expresses the $L$-function at the central point, where (1.1) does not converge, in terms of essentially finite sums of the form resembling a truncated version of Dirichlet series like (1.1). This is standard so we do not reproduce the entire proof.

**Lemma 2.2.** For a primitive Dirichlet character $\chi$ modulo $q$, let $\kappa \in \{0, 1\}$ be such that $\chi(-1) = (-1)^{\kappa}$, and let

$$V(x) = \frac{1}{2\pi i} \int_{(2)} \frac{\Gamma(\frac{s+2}{4} + \frac{1}{2})^2}{\Gamma(\frac{s}{2} + \frac{1}{4})^2} (\pi x)^{-s} ds. \tag{2.1}$$

We have that

$$V(x) \ll_N \min\{1, x^{-N}\} \tag{2.2}$$

for any $x, N > 0$, and

$$|L(\frac{1}{2}, \chi)|^2 = 2 \sum_{nm \geq 1} \frac{\chi(n)\overline{\chi}(m)}{(nm)^{\frac{1}{2}}} V\left(\frac{nm}{q}\right). \tag{2.3}$$

**Proof.** See [9, Lemma 2.1]. For the estimate (2.2), shift the line of integration to $\Re(s) = N$ if $x > 1$, and to $\Re(s) = -\frac{1}{4}$ if $x \leq 1$. The shift left crosses a simple pole at $s = 0$, with residue 1. \hfill $\square$

By the decay property (2.2), the range of summation in the sum (2.3) is essentially $nm < q^{1+\epsilon}$. Note that the sum is restricted to $(nm, p) = 1$, for otherwise the character values vanish.

We conclude the preliminaries section with two known results in elementary number theory. The first of these, Hensel's lemma, describes solutions to polynomial congruences modulo prime powers. In Lemma 2.3, we have taken the first statement from [15, Theorem 4.15(i)], and the second one follows by induction on $k$.

**Lemma 2.3** (Hensel's Lemma). Suppose that $f(x)$ is a polynomial with integer coefficients, $k$ is an integer with $k \geq 2$, and $p$ is a prime.

1. If $r$ is a solution of the congruence $f(x) \equiv 0 \pmod{p^{k-1}}$ such that $f'(r) \not\equiv 0 \pmod{p}$, then there is a unique integer $t$, $0 \leq t < p$, such that $f(r + tp^{k-1}) \equiv 0 \pmod{p^k}$.

2. If $r$ is a solution of the congruence $f(x) \equiv 0 \pmod{p^k}$ such that $f'(r) \not\equiv 0 \pmod{p}$, then there is a unique integer $t$, $0 \leq t < p^k$, such that $t \equiv r \pmod{p}$ and $f(t) \equiv 0 \pmod{p^k}$.

The second number-theoretic result we record is concerned with the number of ways certain definite quadratic forms such as $n^2 + m^2$ in two integers $n, m$ can take the same value.

**Lemma 2.4.** Let $q(n, m)$ be any of $n^2 + m^2$, $n^2 + nm + m^2$, or $n^2 - nm + m^2$. Then, for every $\epsilon > 0$,

$$r_q(N) := \#\{(n, m) \in \mathbb{Z}^2 : q(n, m) = N\} \ll_{\epsilon} N^\epsilon.$$

For $q_0(n, m) = n^2 + m^2$, the estimate $r_{q_0}(N) \ll_{\epsilon} N^\epsilon$ follows from the famous theorem of Gauss for the number of representations of a positive integer $N$ as the sum of two squares [15, Theorem 14.13]: if $N$ has a canonical prime power factorization as $N = 2^{a_0}p_1^{e_1} \cdots p_s^{e_s}q_1^{f_1} \cdots q_t^{f_t}$, where primes $p_i$ are of the form $4k + 1$ and primes $q_j$ are of the form $4k + 3$, then

$$r_{q_0}(N) = 4(e_1 + 1)(e_2 + 1) \cdots (e_s + 1)$$

if all $f_j$ are even, and $r_{q_0}(N) = 0$ otherwise. In particular, $r_{q_0}(N)$ is bounded by the number of divisors $\tau(N)$ as $r_{q_0}(N) \leq 4\tau(N)$, hence $r_{q_0}(N) \ll_{\epsilon} N^\epsilon$ by the standard divisor bound (see, for example, [17, Section 3.5], [7, (12.82)]).

Gauss' formula for $r_{q_0}(N)$ can be proved using the arithmetic of the ring of Gaussian integers $\mathbb{Z}[i]$. This is a Euclidean domain (relative to the usual norm) and hence a unique factorization domain, in which 2 is the sole ramified prime, rational primes of the form $4k + 1$ split as the product of two distinct conjugate Gaussian primes, and rational primes of the form $4k + 3$ remain as Gaussian
primes [15, Theorem 14.12]. A similar argument could be made for \( q_1(n, m) = n^2 + nm + m^2 \) and
\( q_2(n, m) = n^2 - nm + m^2 \) by using the arithmetic of the ring of Eisenstein integers \( \mathbb{Z}[\omega] \), where \( \omega = \frac{-1}{2} + i\frac{\sqrt{3}}{2} \) is a primitive cube root of unity, and by distinguishing between primes of the form \( 6k + 1 \) and \( 6k + 5 \). In each of these cases, unique factorization allows for very pretty formulas for \( r_q(N) \); however, this is ultimately not so important if all we need is the upper bound of Lemma 2.4.

To make this clear, we provide a streamlined argument that applies in more general situations.

Proof. Note that, if \( N = n^2 + m^2 = (n + mi)(n - mi) \), then \( (n + mi) \mid N \) in the ring \( \mathbb{Z}[i] \).
Similarly, if \( N = n^2 - nm + m^2 = (n + m\omega)(n + m\omega^2) \), then \( (n + m\omega) \mid N \) in \( \mathbb{Z}[\omega] \), and if
\( N = n^2 + nm + m^2 = (n - m\omega)(n - m\omega^2) \), then \( (n - m\omega) \mid N \) in \( \mathbb{Z}[\omega] \). Therefore, denoting \( F = \mathbb{Q}(i) \) if \( q(n, m) = n^2 + m^2 \) and \( F = \mathbb{Q}(\omega) \) if \( q(n, m) = n^2 \pm nm + m^2 \), we have that

\[ r_q(N) \ll \tau_F(N). \]

Here, \( \tau_F(N) \) denotes the number of ideal divisors of the ideal \( (N) = NO_F \) in the ring of integers \( O_F \) of \( F \), and the absolute implied constant accounts for the finite group of units, which, in this case, are all roots of unity. Therefore the desired estimate follows from the following divisor bound in terms of the absolute ideal norm:

\[ \tau_F(n) \ll \mathfrak{N}n^\epsilon, \]

which is valid in any number field \( F \) (with a constant possibly depending on \( F \)).

The estimate (2.4) can be proved for any number field \( F \) along the same lines as over \( \mathbb{Q} \) [17, Section 3.5]. It is clear that

\[ \tau_F(p^\alpha) = \alpha + 1 \leq (\mathfrak{N}p^\alpha)^\epsilon = \mathfrak{N}p^{\alpha\epsilon} \]

for all prime powers \( p^\alpha \) with \( \alpha \geq 1 \) and sufficiently large \( \mathfrak{N}p \) (say, \( \mathfrak{N}p \geq 2^{1/\epsilon} \)). A similar inequality holds, by allowing for a larger (but fixed once and for all for a given \( F \)) implied constant, for powers of the finitely many prime ideals with \( \mathfrak{N}p < 2^{1/\epsilon} \). The estimate (2.4) follows by multiplicativity. \( \square \)

3. The diagonal contribution

Writing the sum in (2.3) as the sum of terms with \( n = m \) plus the sum of terms with \( n \neq m \), we get

\[ \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} |L(\frac{1}{2}, \chi)|^2 = \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} \left( 2 \sum_{n \geq 1} \frac{1}{n} V\left( \frac{n^2}{q} \right) \right) + \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} \left( 2 \sum_{n, mn \geq 1 \atop n \neq m} \frac{\chi(n)\overline{\chi}(m)}{(nm)^{2}} V\left( \frac{nm}{q} \right) \right). \]

The first sum above is the ‘diagonal’ and it forms the main term of Theorem 1.1. This is not surprising because there are no character values in the sum, so the sum over characters on the outside cannot produce any cancellation. By [9, Section 3.3] we have

\[ \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} \left( 2 \sum_{n \geq 1} \frac{1}{n} V\left( \frac{n^2}{q} \right) \right) = \frac{p - 1}{p} (\log q + C) + O(q^{-1/2+\epsilon}). \]

We recall that this argument uses the integral representation (2.1) and contour shifting and is fully effective.

Now it remains to bound the second sum of (3.1). This will be the dominant part of the error term in Theorem 1.1.
4. The off-diagonal contribution

Applying Lemma 2.1 and (2.2), we get
\[
\frac{1}{|O|} \sum_{\chi \in O} \left( 2 \sum_{\substack{nm \geq 1 \\ n \neq m}} \chi(nm) \overline{\chi}(m) V \left( \frac{nm}{q} \right) \right) \ll \sum_{nm \leq q^{1+\epsilon}} \frac{1}{(nm)^{\frac{1}{2}}} + q^{-100}.
\]

We will analyze this sum in dyadic intervals
\[
N \leq n < 2N, \quad M \leq m < 2M,
\]
where
\[
NM < q^{1+\epsilon}.
\]

Since there are at most \( q^\epsilon \) such dyadic intervals, the task is reduced to bounding
\[
S_p = S_p(N, M) := \frac{1}{(NM)^{\frac{1}{2}}} \sum_{\substack{N \leq n < 2N \\ M \leq m < 2M \\ nm \neq q \mod p^{k-1}}} 1;
\]
for a proof of Theorem 1.1, we require the bound \( S_p \ll q^{-\lambda_0 + \epsilon} \) in the range (4.1). Let us first note a ‘trivial’ bound (this argument is from [9, Section 3.3]).

Lemma 4.1. We have
\[
S_p \ll \min \left\{ \left( \frac{N}{M} \right)^{1/2}, \left( \frac{M}{N} \right)^{1/2} \right\} + q^{-1/2 + \epsilon}
\]
and
\[
S_p \ll \min \left\{ q^{1/2} \frac{M}{N}, q^{1/2} \frac{N}{M} \right\} + q^{-1/2 + \epsilon}.
\]

Proof. Suppose without loss of generality that \( N \leq M \). For each of the \( N \) choices of \( n \) in the sum \( S_p \), the value of \( m^{p-1} \) is uniquely determined modulo \( p^{k-1} \), namely, \( m^{p-1} \equiv n^{p-1} \pmod{p^{k-1}} \). By Lemma 2.3 (2) with \( f(x) = x^{p-1} - n^{p-1} \), for every \( m_0 \pmod{p} \), \( (m_0, p) = 1 \), there is a unique value of \( m \) modulo \( p^{k-1} \) such that \( m \equiv m_0 \pmod{p} \) and \( f(m) \equiv 0 \pmod{p^{k-1}} \). Therefore, once the value of \( n \) in \( S_p \) has been fixed, there are at most \( O(1) \) choices for the congruence class of \( m \pmod{p^{k-1}} \), and thus there are at most \( O(M/q + 1) \) choices for \( m \) itself. So the sum \( S_p \) is bounded as
\[
S_p \ll \frac{1}{(NM)^{1/2}} \cdot N \cdot \left( \frac{M}{q} + 1 \right).
\]

This gives the bound (4.2) on using (4.1). The bound (4.3) follows from (4.2) by using (4.1) again. \( \square \)

We can see that the bound of Lemma 4.1 is sufficient as long as the sizes of \( N \) and \( M \) are apart by a certain power of \( q \). From this point onwards, our argument differs from that of [9].

4.1. The case \( p = 3 \). The sum we need to bound is
\[
S_3 = \frac{1}{(NM)^{1/2}} \sum_{\substack{N \leq n < 2N \\ M \leq m < 2M \\ nm \neq q \mod 3^{k-1}}} 1.
\]

The congruence condition of \( S_3 \) implies that \( 3^{k-1} \) divides \( (n - m)(n + m) \). Since \( (nm, 3) = 1 \), we know that \( n - m \) and \( n + m \) are not both divisible by 3 (for if they were, their sum would be too and this would lead to a contradiction). This means that either \( 3^{k-1} \) divides \( n - m \), or \( 3^{k-1} \) divides \( n + m \). We also have the condition \( n \neq m \). So we must have that at least one of \( N \) and \( M \) is at least
as large as $3^k - 1$, lest $n - m$ and $n + m$ be too small to satisfy the divisibility condition. Thus by (4.3) we get

$$S_n \ll q^{-1/2+\epsilon}.$$  

4.2. The case $p = 5$. The sum we need to bound is

$$S_5 = \sum_{\substack{N \leq n < 2N \\ M \leq m < 2M \\ (nm, 5) = 1, n \neq m \\ n^2 \equiv m^2 \mod 5^{k-1}}} \frac{1}{(NM)^{\frac{1}{2}}}. \tag{4.4}$$

Suppose without loss of generality that $M \geq N$. The congruence condition of $S_5$ implies that $5^{k-1}$ divides $(n^2 - m^2)(n^2 + m^2)$. Since $(nm, 5) = 1$, we know that $n^2 - m^2$ and $n^2 + m^2$ are not both divisible by 5 (for if they were, their sum would be too and this would lead to a contradiction). Thus $5^{k-1}$ divides either $n^2 - m^2$ or $n^2 + m^2$. The subsum of $S_5$ consisting of terms satisfying $5^{k-1} \mid (n^2 - m^2)$ is $O(q^{-1/2+\epsilon})$ by the argument given for $p = 3$.

Consider the terms satisfying $5^{k-1} \mid (n^2 + m^2)$. First note that we must have $M \gg q^{1/2}$ or else $n^2 + m^2$ is too small to satisfy the divisibility. Now, writing

$$n^2 + m^2 = 5^{k-1}h,$$

we see that $h \ll M^2/q$. By Lemma 2.4, for each choice of $h$, there are $O(q^\epsilon)$ choices for $n$ and $m$. So there are at most $q^\epsilon(M^2/q)$ summands satisfying $5^{k-1} \mid (n^2 + m^2)$ in (4.4). We get

$$S_5 \ll q^{-1/2+\epsilon} + \frac{1}{(NM)^{\frac{1}{2}}} \frac{M^2}{q^{1-\epsilon}} \ll q^{-1/2+\epsilon} + \left(\frac{M}{N}\right)^{1/2} \frac{M}{q^{1-\epsilon}}. \tag{4.5}$$

Now we consider two cases: when $N$ and $M$ are quite close and when they are not.

Suppose that $M/N < q^{1/3}$. Then by (4.1) we have $M^2 \ll (M/N)q^{1+\epsilon} \ll q^{4/3+\epsilon}$. So (4.5) becomes

$$S_5 \ll q^{-1/6+\epsilon}. \tag{4.6}$$

Now suppose that $M/N \geq q^{1/3}$. Then by (4.2), we get the same bound (4.6).

4.3. The case $p = 7$. The sum we need to bound is

$$S_7 = \sum_{\substack{N \leq n < 2N \\ M \leq m < 2M \\ (nm, 7) = 1, n \neq m \\ n^2 \equiv m^2 \mod 7^{k-1}}} \frac{1}{(NM)^{\frac{1}{2}}} \tag{4.7}.$$  

The congruence condition of $S_7$ implies that

$$7^{k-1} \mid (n^2 - m^2)(n^2 + nm + m^2)(n^2 - nm + m^2).$$

Since $(nm, 7) = 1$, we get that 7 cannot divide more than one factor on the right hand side. For example, if $7 \mid (n^2 - m^2)$ then $n \equiv \pm m \mod 7$. So if also $7 \mid (n^2 + nm + m^2)$, then $7 \mid (n^2 \pm n^2 + n^2)$, which is impossible. So we have the cases $7^{k-1} \mid (n^2 - m^2)$ or $7^{k-1} \mid (n^2 \pm nm + m^2)$. Now by the same argument as for $p = 5$, we get

$$S_7 \ll q^{-1/6+\epsilon}.$$
References


Science Program, Texas A&M University at Qatar, PO Box 23874, Doha, Qatar
E-mail address: rizwanur.khan@qatar.tamu.edu

North Miami Beach, FL 33162
E-mail address: rlei@brynmawr.edu

Department of Mathematics, Bryn Mawr College, 101 North Merion Avenue, Bryn Mawr, PA 19010
E-mail address: dmilicevic@brynmawr.edu