

# involve

a journal of mathematics

## Effective moments of Dirichlet $L$ -functions in Galois orbits

Rizwanur Khan, Ruoyun Lei and Djordje Milićević



# Effective moments of Dirichlet $L$ -functions in Galois orbits

Rizwanur Khan, Ruoyun Lei and Djordje Milićević

(Communicated by Stephan Garcia)

Khan, Milićević, 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 [Davenport 2000] for further background), the associated  $L$ -function is defined for  $\operatorname{Re}(s) > 1$  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

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

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

$$\kappa := \begin{cases} 0 & \text{if } \chi(-1) = 1, \\ 1 & \text{if } \chi(-1) = -1. \end{cases} \quad (1-2)$$

MSC2010: 11M20.

Keywords:  $L$ -functions, Dirichlet characters, moments.

As is typically the case, the line of symmetry  $\operatorname{Re}(s) = \frac{1}{2}$  of the functional equation is where the  $L$ -function is most difficult to understand. Since the values at  $s = \frac{1}{2}$  of  $L$ -functions 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 [Bui 2012; Khan and Ngo 2016; Soundararajan 2000]. As another example, an analog of the Lindelöf conjecture asserts that  $L(\frac{1}{2}, \chi) \ll q^\epsilon$  for any  $\epsilon > 0$ , but again only partial results exist [Burgess 1963; Conrey and Iwaniec 2000; Milićević 2016]. (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  $L(\frac{1}{2}, \chi)$  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, [Katz and Sarnak 1999].

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

$$\sum_{\chi \bmod q}^* L(\tfrac{1}{2}, \chi)^n$$

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

$$\sum_{\chi \bmod q}^* |L(\tfrac{1}{2}, \chi)|^n$$

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 [1931]. The third and fourth moments ( $n = 3, 4$ ) are quite recent. The third moment was obtained by Zacharias [2017] for prime values of  $q$ . The fourth moment was first obtained by Heath-Brown [1981] for values of  $q$  with a

restricted number of prime factors and by Soundararajan [2007] for all values of  $q$ , and an asymptotic with a power savings error term was given by Young [2011] for prime values of  $q$ ; see also [Blomer and Milićević 2015] for factorable  $q$  (including prime powers). No asymptotic is known for the fifth moment or higher ( $n \geq 5$ ).

In this paper we are interested in moments over natural subsets of the primitive Dirichlet characters 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 “harmonics” 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.

Several works have studied the average values of  $L$ -functions over these orbits [Chinta 2002; Greenberg 1985; Khan et al. 2016; Rohrlich 1984]. For the rest of the paper, we specialize to moduli of the form

$$q = p^k,$$

where  $p$  is a fixed odd prime (thus  $q \rightarrow \infty$  is equivalent to  $k \rightarrow \infty$ ). 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  $d \mid (p-1)$ , and the primitive characters of order  $l$  form an orbit  $\mathcal{O}$  of cardinality  $\phi(l)$ ; see Table 1 for an example. These facts are justified in [Khan et al. 2016].

In the course of studying nonvanishing of Dirichlet  $L$ -functions within the Galois orbits described above, Ngo and two of us proved in [Khan et al. 2016, Theorem 1.2b] the following asymptotic for the second moment (as  $k \rightarrow \infty$ ): for any given orbit  $\mathcal{O}$  and  $\epsilon > 0$ , we have

$$\frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} |L(\tfrac{1}{2}, \chi)|^2 = \frac{p-1}{p} (\log q + C) + O(q^{-1/4+\epsilon}), \quad (1-3)$$

where

$$C = \frac{\Gamma'(\frac{1}{4}(1+2\kappa))}{\Gamma(\frac{1}{4}(1+2\kappa))} + 2\gamma + 2\frac{\log p}{p-1} - \log \pi,$$

$\log$  is the natural logarithm,  $\gamma = 0.57721 \dots$  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

$n \bmod 9$	1	2	4	5	7	8	primitive?	order	orbit
$\chi_0(n)$	1	1	1	1	1	1		1	$\{\chi_0\}$
$\chi_1(n)$	1	$\xi$	$\xi^2$	$\xi^5$	$\xi^4$	$-1$	$\checkmark$	$3 \cdot 2$	$\{\chi_1, \chi_5\}$
$\chi_2(n)$	1	$\xi^2$	$\xi^4$	$\xi^4$	$\xi^2$	1	$\checkmark$	$3 \cdot 1$	$\{\chi_2, \chi_4\}$
$\chi_3(n)$	1	$-1$	1	$-1$	1	$-1$		2	$\{\chi_3\}$
$\chi_4(n)$	1	$\xi^4$	$\xi^2$	$\xi^2$	$\xi^4$	1	$\checkmark$	$3 \cdot 1$	$\{\chi_2, \chi_4\}$
$\chi_5(n)$	1	$\xi^5$	$\xi^4$	$\xi$	$\xi^2$	$-1$	$\checkmark$	$3 \cdot 2$	$\{\chi_1, \chi_5\}$

**Table 1.** Four of the six characters modulo  $9 = 3^2$  are primitive. They fall into two Galois orbits, the orbit  $\{\chi_2, \chi_4\}$  consisting of characters of order  $3 \cdot 1 = 3$ , of size  $\phi(3) = 2$ , and the orbit  $\{\chi_1, \chi_5\}$  consisting of characters of order  $3 \cdot 2 = 6$ , of size  $\phi(6) = 2$ .

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 [Khan et al. 2016] hinges crucially on Roth’s theorem in Diophantine approximation (more precisely, on the  $p$ -adic version of Roth’s theorem due to Ridout [1958]), 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  $\mathcal{O}$  of characters modulo  $q$ , we have*

$$\frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} \left| L\left(\frac{1}{2}, \chi\right) \right|^2 = \frac{p-1}{p} (\log q + C) + O(q^{-\lambda_p + \epsilon}),$$

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

Our argument differs from that of [Khan et al. 2016] in that we do not appeal to Roth’s theorem. The present argument yields the fully effective Theorem 1.1 (with computable bounds on the error term), and in fact in (5-11) we provide an explicit version with a specific constant depending on  $\epsilon > 0$ . 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 [Khan et al. 2016, 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  $\epsilon$ .

## 2. Preliminaries

We first state a result which follows directly from [\[Khan et al. 2016, Lemma 2.3\]](#). This illustrates an orthogonality property within orbits.

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

$$n^{p-1} \not\equiv m^{p-1} \pmod{p^{k-1}},$$

then

$$\frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} \chi(n) \bar{\chi}(m) = 0.$$

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*

$$V(x) = \frac{1}{2\pi i} \int_{(2)} \frac{\Gamma\left(\frac{1}{2}(s + \kappa) + \frac{1}{4}\right)^2}{\Gamma\left(\frac{1}{2}\kappa + \frac{1}{4}\right)^2} (\pi x)^{-s} \frac{ds}{s}. \quad (2-1)$$

We have

$$V(x) \ll_N \min\{1, x^{-N}\} \quad (2-2)$$

for any  $x, N > 0$ , and

$$\left| L\left(\frac{1}{2}, \chi\right) \right|^2 = 2 \sum_{nm \geq 1} \frac{\chi(n) \bar{\chi}(m)}{(nm)^{1/2}} V\left(\frac{nm}{q}\right). \quad (2-3)$$

*Proof.* See [\[Khan et al. 2016, Lemma 2.1\]](#). For the estimate (2-2), shift the line of integration to  $\operatorname{Re}(s) = N$  if  $x > 1$ , and to  $\operatorname{Re}(s) = -\frac{1}{4}$  if  $x \leq 1$ . The shift left crosses a simple pole at  $s = 0$ , with residue 1.  $\square$

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 [\[Rosen 1984, 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  $f(x) \equiv 0 \pmod{p}$  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 [\[Rosen 1984, Theorem 14.13\]](#): if  $N$  has a canonical prime power factorization as  $N = 2^m p_1^{e_1} \cdots p_s^{e_s} q_1^{f_1} \cdots q_t^{f_t}$ , 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, [\[Stopple 2003, Section 3.5; Iwaniec and Kowalski 2004, \(12.82\)\]](#).

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 [\[Rosen 1984, Theorem 14.12\]](#). 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, writing  $F = \mathbb{Q}(i)$  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

$$r_q(N) \ll \tau_F(N).$$

Here,  $\tau_F(N)$  denotes the number of ideal divisors of the ideal  $(N) = N\mathcal{O}_F$  in the ring of integers  $\mathcal{O}_F$  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 divisor bound

$$\tau_F(\mathfrak{n}) \ll_{\epsilon} \mathfrak{N}\mathfrak{n}^{\epsilon} \quad (2-4)$$

in terms of the absolute ideal norm, 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  $\mathbb{Q}$  [[Stoppole 2003](#), Section 3.5]. It is clear that

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

for all prime powers  $\mathfrak{p}^{\alpha}$  with  $\alpha \geq 1$  and sufficiently large  $\mathfrak{N}\mathfrak{p}$  (say,  $\mathfrak{N}\mathfrak{p} \geq e^{1/\epsilon}$ ). 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  $\mathfrak{N}\mathfrak{p} < 2^{1/\epsilon}$ . 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

$$\begin{aligned} \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} |L(\tfrac{1}{2}, \chi)|^2 &= \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} \left( 2 \sum_{\substack{n \geq 1 \\ (n, p)=1}} \frac{1}{n} V\left(\frac{n^2}{q}\right) \right) \\ &\quad + \frac{1}{|\mathcal{O}|} \sum_{\substack{\chi \in \mathcal{O} \\ nm \geq 1 \\ n \neq m}} \left( 2 \sum_{\substack{\chi(n) \bar{\chi}(m) \\ (nm)^{\frac{1}{2}}}} V\left(\frac{nm}{q}\right) \right). \end{aligned} \quad (3-1)$$

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 [Khan et al. 2016, Section 3.3] we have

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

We recall that this argument uses the integral representation (2-1) and contour shifting and is fully effective.

Now it remains to bound the off-diagonal 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

$$\frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} \left( 2 \sum_{\substack{nm \geq 1 \\ n \neq m}} \frac{\chi(n) \bar{\chi}(m)}{(nm)^{1/2}} V\left(\frac{nm}{q}\right) \right) \ll \sum_{\substack{nm < q^{1+\epsilon} \\ (nm, p) = 1, n \neq m \\ n^{p-1} \equiv m^{p-1} \pmod{p^{k-1}}}} \frac{1}{(nm)^{1/2}} + q^{-100}.$$

We will analyze this sum in dyadic intervals

$$N \leq n < 2N, \quad M \leq m < 2M,$$

where

$$NM < q^{1+\epsilon}. \tag{4-1}$$

Since there are at most  $q^\epsilon$  such dyadic intervals, the task is reduced to bounding

$$\mathcal{S}_p = \mathcal{S}_p(N, M) := \frac{1}{(NM)^{1/2}} \sum_{\substack{N \leq n < 2N \\ M \leq m < 2M \\ (nm, p) = 1, n \neq m \\ n^{p-1} \equiv m^{p-1} \pmod{p^{k-1}}}} 1;$$

for a proof of Theorem 1.1, we require the bound  $\mathcal{S}_p \ll q^{-\lambda_p + \epsilon}$  in the range (4-1). Let us first note a “trivial” bound (this argument is from [Khan et al. 2016, Section 3.3]).

**Lemma 4.1.** *We have*

$$\mathcal{S}_p \ll \min \left\{ \left( \frac{N}{M} \right)^{1/2}, \left( \frac{M}{N} \right)^{1/2} \right\} + q^{-1/2+\epsilon}, \tag{4-2}$$

$$\mathcal{S}_p \ll \min \left\{ \frac{q^{1/2+\epsilon}}{M}, \frac{q^{1/2+\epsilon}}{N} \right\} + q^{-1/2+\epsilon}. \tag{4-3}$$

*Proof.* Suppose without loss of generality that  $N \leq M$ . For each of the  $N$  choices of  $n$  in the sum  $\mathcal{S}_p$ , 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  $\mathcal{S}_p$  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  $\mathcal{S}_p$  is bounded as

$$\mathcal{S}_p \ll \frac{1}{(NM)^{1/2}} \cdot N \cdot \left( \frac{M}{q} + 1 \right).$$

This gives the bound (4-2) by 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 [Khan et al. 2016].

**4.1. The case  $p = 3$ .** The sum we need to bound is

$$\mathcal{S}_3 = \frac{1}{(NM)^{1/2}} \sum_{\substack{N \leq n < 2N \\ M \leq m < 2M \\ (nm, 3) = 1, n \neq m \\ n^2 \equiv m^2 \pmod{3^{k-1}}}} 1.$$

The congruence condition of  $\mathcal{S}_3$  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  $3^{k-1}/4$ , lest  $n - m$  and  $n + m$  be too small to satisfy the divisibility condition. Thus by (4-3) we get

$$\mathcal{S}_3 \ll q^{-1/2+\epsilon}.$$

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

$$\mathcal{S}_5 = \frac{1}{(NM)^{1/2}} \sum_{\substack{N \leq n < 2N \\ M \leq m < 2M \\ (nm, 5) = 1, n \neq m \\ n^4 \equiv m^4 \pmod{5^{k-1}}}} 1. \quad (4-4)$$

Suppose without loss of generality that  $M \geq N$ . The congruence condition of  $\mathcal{S}_5$  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

$$S_5 \ll q^{-1/2+\epsilon} + \frac{1}{(NM)^{1/2}} \frac{M^2}{q^{1-\epsilon}} \ll q^{-1/2+\epsilon} + \left(\frac{M}{N}\right)^{1/2} \frac{M}{q^{1-\epsilon}}. \quad (4-5)$$

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

$$S_5 \ll q^{-1/6+\epsilon}. \quad (4-6)$$

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

$$S_7 = \frac{1}{(NM)^{1/2}} \sum_{\substack{N \leq n < 2N \\ M \leq m < 2M \\ (nm, 7)=1, n \neq m \\ n^6 \equiv m^6 \pmod{7^{k-1}}} 1.$$

The congruence condition of  $S_7$  implies

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

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  $n \equiv \pm m \pmod{7}$ . So if also  $7 \mid (n^2 \pm nm + m^2)$ , then  $7 \mid (n^2 \pm n^2 + n^2)$ , which is impossible. On the other hand, if  $7 \mid (n^2 + nm + m^2)$  and  $7 \mid (n^2 - nm + m^2)$ , then  $7 \mid nm$ , which is again impossible. So we have the cases  $7^{k-1} \mid (n^2 - m^2)$  or  $7^{k-1} \mid (n^2 \pm nm + m^2)$ . By the argument given for  $p = 3$ , the subsum of  $S_7$  consisting of terms satisfying  $7^{k-1} \mid (n^2 - m^2)$  is  $O(q^{-1/2+\epsilon})$ .

For the cases when  $7^{k-1} \mid (n^2 \pm nm + m^2)$ , we proceed analogously to the case  $p = 5$ . We must have  $M \gg q^{1/2}$  or else  $n^2 \pm nm + m^2$  is too small to be divisible by  $7^{k-1}$ , and in fact  $n^2 \pm nm + m^2 = 7^{k-1}h$  for some  $h \ll M^2/q$ . By Lemma 2.4 (this time applied with the form  $n^2 \pm nm + m^2$ ), the number of choices of  $(n, m)$  is  $O(q^\epsilon)$  for each choice of  $h$  and thus at most  $q^\epsilon (M^2/q)$  altogether. Therefore,

$$S_7 \ll q^{-1/2+\epsilon} + \frac{1}{(NM)^{1/2}} \frac{M^2}{q^{1-\epsilon}} \ll q^{-1/2+\epsilon} + \left(\frac{M}{N}\right)^{1/2} \frac{M}{q^{1-\epsilon}}.$$

Using this bound and (4-1) when  $M/N < q^{1/3}$  and (4-2) when  $M/N \geq q^{1/3}$ , we obtain

$$\mathcal{S}_7 \ll q^{-1/6+\epsilon}.$$

## 5. Effective estimates

In this section, we show how all the estimates of previous sections can be made fully effective for any desired choice of  $\epsilon > 0$ . We follow the exposition in Sections 2–4 and indicate explicit constants at each place. Since many of these computations are routine, we condense some of the details but provide all the essential steps.

**5.1. Preliminaries.** When estimating expressions involving  $\Gamma(s)$ , we use the following well-known facts valid for  $\sigma = \operatorname{Re} s > 0$  and integers  $N \geq 2$ :

$$\begin{aligned} \Gamma(s) &= \frac{1}{s} \Gamma(s+1), \quad \Gamma(s) \Gamma\left(s + \frac{1}{2}\right) = 2^{1-2s} \sqrt{\pi} \Gamma(2s), \quad |\Gamma(s)| \leq \Gamma(\sigma), \\ |\Gamma(\sigma + \tfrac{1}{4}) \Gamma(\sigma + \tfrac{5}{4})| &\leq |\Gamma(\sigma) \Gamma(\sigma + \tfrac{3}{2})|, \quad |\Gamma(N)| \leq \tfrac{1}{4} e^2 (N/e)^N. \end{aligned} \quad (5-1)$$

The first inequality in the second row follows from the convexity of  $\log \Gamma(\sigma)$ , and the second one follows by using integral comparison to estimate  $\sum_{n \leq N} \log n$ .

In Lemma 2.2, for  $\kappa = 0$ , we find by shifting contours to  $\operatorname{Re} s = N \geq 3$  that

$$\begin{aligned} |V(x)| &\leq \frac{1}{2\pi \Gamma(\frac{1}{4})^2} \Gamma(\tfrac{1}{2}N + \tfrac{1}{4}) \Gamma(\tfrac{1}{2}N + \tfrac{5}{4}) \int_{-\infty}^{\infty} \frac{dt}{|\tfrac{1}{2}(N+it) + \tfrac{1}{4}| |N+it|} \cdot (\pi x)^{-N} \\ &\leq \frac{\sqrt{\pi}}{2\pi \Gamma(\frac{1}{4})^2} \cdot (N+1) \Gamma(N) (2\pi)^{-N} \cdot \frac{8}{N} \cdot x^{-N} < \frac{3}{4} \left(\frac{N}{2\pi e}\right)^N \cdot x^{-N}, \end{aligned}$$

where the integral is split into  $|t| \leq N$  and  $|t| > N$  and then estimated trivially. Similarly, by shifting to  $\operatorname{Re} s = -\frac{1}{4}$ ,

$$|V(x) - 1| \leq \frac{\pi^{1/4} \Gamma(\frac{1}{8}) \Gamma(\frac{7}{8})}{2\pi \Gamma(\frac{1}{4})^2} \int_{-\infty}^{\infty} \frac{dt}{|\frac{1}{8} + \frac{1}{2}it| |-\frac{1}{4} + it|} \cdot x^{1/4} < 3x^{1/4},$$

where the integral is  $\leq 16\sqrt{2}$  by splitting into  $|t| \leq \frac{1}{2\sqrt{2}}$  and  $|t| > \frac{1}{2\sqrt{2}}$  and estimating trivially. One similarly verifies that the same upper bounds hold for  $\kappa = 1$ . Using the first bound for  $x \geq N/(2\pi e)$  and the second one for  $x < N/(2\pi e)$ , we obtain for  $N \geq 3$

$$|V(x)| \leq \min \left\{ \frac{5N^{1/4}}{2}, \frac{3}{4} \left(\frac{N}{2\pi e}\right)^N \cdot x^{-N} \right\}. \quad (5-2)$$

Next, we make (2-4) effective. Since the group of units in an imaginary quadratic number field such as  $F = \mathbb{Q}(i)$  or  $F = \mathbb{Q}(\omega)$  is a cyclic group of order at most 6, it is easy to see that  $r_q(N) \leq 3 \cdot \tau_F(N)$ . For a prime ideal  $\mathfrak{p}$  with  $\mathfrak{N}\mathfrak{p} \geq e^{1/\epsilon}$ , we simply have  $\tau_F(\mathfrak{p}^\alpha) = 1 + \alpha \leq (\mathfrak{N}\mathfrak{p}^\alpha)^\epsilon$ . For the remaining primes, the function

$F(\alpha) = \mathfrak{N}\mathfrak{p}^{\alpha\epsilon}/(1+\alpha)$  has a minimum at  $\alpha_0 = 1/(\epsilon \log \mathfrak{N}\mathfrak{p}) - 1 > 0$  with  $F(\alpha_0) \geq e\epsilon \log \mathfrak{N}\mathfrak{p}/\mathfrak{N}\mathfrak{p}^\epsilon$ . Therefore, for every integral ideal  $\mathfrak{n} \subseteq \mathcal{O}_F$ ,

$$\frac{\tau_F(\mathfrak{n})}{\mathfrak{N}\mathfrak{n}^\epsilon} \leq \prod_{\mathfrak{N}\mathfrak{p} \leq e^{1/\epsilon}} \left( e^\epsilon \frac{\log \mathfrak{N}\mathfrak{p}}{\mathfrak{N}\mathfrak{p}^\epsilon} \right)^{-1} \leq \frac{\epsilon^{-2\pi(e^{1/\epsilon})}}{\log 2},$$

where  $\pi(x) = \#\{p \leq x\}$  is the classical prime-counting function, and the number of prime ideals  $\mathfrak{p}$  with  $\mathfrak{N}\mathfrak{p} \leq x$  is clearly  $\leq 2\pi(x)$ . Using the explicit estimate  $\pi(x) \leq 2x/\log x$  [Stopple 2003, Section 5.2], we thus find that, for  $\epsilon \leq \frac{1}{2}$ ,

$$\tau_F(\mathfrak{n}) \leq \frac{e^{4\epsilon|\log \epsilon|e^{1/\epsilon}}}{\log 2} \cdot \mathfrak{N}\mathfrak{n}^\epsilon \leq e^{(3/2)e^{1/\epsilon}} \cdot \mathfrak{N}\mathfrak{n}^\epsilon. \quad (5-3)$$

**5.2. Diagonal terms.** Proceeding to the evaluation of the diagonal contribution in Section 3, following [Khan et al. 2016, Section 3.3], we substitute the integral representation for  $V(x)$  and exchange the order of summation and integration to find that the diagonal contribution equals, for  $\kappa = 0$ ,

$$\frac{1}{2\pi i} \int_{(2)} \zeta_p(2s+1) \frac{\Gamma(\frac{1}{2}s + \frac{1}{4})^2}{\Gamma(\frac{1}{4})^2} \left(\frac{q}{\pi}\right)^s \frac{ds}{s}.$$

We evaluate the integral by shifting to  $\operatorname{Re} s = -\frac{1}{2} + \epsilon$ , collecting the residue from the double pole at  $s = 0$ . We can use a simple estimate for  $\zeta(s)$  with  $0 < \sigma \leq \frac{1}{2}$  as

$$|(1 - 2^{1-s})\zeta(s)| = \left| \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s} \right| \leq \sum_{n=1}^{\infty} |s|(2n-1)^{-\sigma-1} \leq |s| \left(1 + \frac{1}{2\sigma}\right) \leq \frac{|s|}{\sigma},$$

by integral comparison. Further,  $|1 - 2^{1-s}| \geq 2^{2/3} - 1 > \frac{1}{2}$  for  $\sigma \leq \frac{1}{3}$  and  $|1 - p^{-s}| \leq \min(|s| \log p, 2)$  for  $p \geq 3$ , so that the remainder from the contour at  $\operatorname{Re} s = -\frac{1}{2} + \epsilon$ , with  $\epsilon \leq \frac{1}{6}$ , is

$$\begin{aligned} &\leq \frac{1}{2\pi} \frac{2}{2\epsilon} \frac{1}{\Gamma(\frac{1}{4})^2} \int_{-\infty}^{\infty} \frac{|2\epsilon + 2it| \min(|2\epsilon + 2it| \log p, 2)}{|\frac{1}{2}(\epsilon + it)|^2} \frac{dt}{|\epsilon + it|} \cdot \left(\frac{q}{\pi}\right)^{-1/2+\epsilon} \\ &\leq \frac{8\sqrt{\pi}}{\pi \Gamma(\frac{1}{4})^2 \epsilon} \cdot 2 \log p \cdot (2 + |\log \epsilon|) \cdot q^{-1/2+\epsilon} < \frac{3}{2} \log p \frac{|\log \epsilon|}{\epsilon} \cdot q^{-1/2+\epsilon}, \quad (5-4) \end{aligned}$$

by splitting the integral into  $|t| \leq \epsilon$ ,  $\epsilon < |t| \leq 1/\log p$ , and  $|t| > 1/\log p$  and estimating trivially. It is similarly verified that this explicit estimate for the error term in the evaluation of the diagonal contribution in Section 3 holds also when  $\kappa = 1$ .

**5.3. Off-diagonal terms.** We now come to the crux of the matter, the estimation of the off-diagonal terms in Section 4, in which  $p \leq 7$  and we may assume that

$0 < \epsilon \leq \lambda_p$ . As a preliminary step, we find that the function  $G(q) = q^\epsilon / \log q$  has a minimum at  $q_0 = e^{1/\epsilon}$  with  $G(q_0) = \epsilon e$ , so that

$$\log q \leq \frac{1}{\epsilon e} \cdot q^\epsilon.$$

For  $x \geq 1$  and  $N \geq 2$ ,

$$\sum_{m \leq x} \frac{1}{m^{N+1/2}} \leq \frac{1}{x^{N-1/2}} \left( \frac{1}{N-\frac{1}{2}} + \frac{1}{x} \right) \leq \frac{2}{x^{N-1/2}}.$$

Using this, the contribution of the terms with  $nm > q^{1+\epsilon}$  is estimated using (5-2) as

$$\begin{aligned} 2 \sum_{nm > q^{1+\epsilon}} \frac{1}{(nm)^{1/2}} V\left(\frac{nm}{q}\right) \\ \leq 4 \frac{3}{4} \left(\frac{N}{2\pi e}\right)^N q^N \left( \sum_{n \leq q^{1/2+\epsilon}} \frac{1}{n^{1/2+N}(q^{1+\epsilon}/n)^{N-1/2}} + \sum_{n > q^{1+\epsilon}} \frac{1}{n^{1/2+N}} \right) \\ \leq 3 \left(\frac{N}{2\pi e}\right)^N \frac{q^{1/2}}{q^{(N-1)\epsilon}} (\log q^{1+\epsilon} + 2) < \frac{4}{\epsilon} \left(\frac{N}{2\pi e}\right)^N \frac{q^{1/2}}{q^{(N-2)\epsilon}} \end{aligned}$$

for  $\epsilon \leq \frac{1}{2}$ . Taking  $N \geq 1/\epsilon + 2$ , the total contribution of terms with  $nm > q^{1+\epsilon}$  is

$$\leq \frac{4}{\epsilon(2\pi e)^{1/\epsilon+2}} (1 + 3\epsilon)^{1/\epsilon+3} \cdot q^{-1/2} < \frac{1}{\epsilon^3(2\pi e)^{1/\epsilon}} \cdot q^{-1/2}. \quad (5-5)$$

The terms with  $nm < q^{1+\epsilon}$  can be split into at most

$$\frac{\log q^{1+\epsilon}}{\log 2} + 1 \leq \frac{7}{6} \frac{1}{\log 2 \cdot e\epsilon} q^\epsilon + 1 < \left(\frac{1}{\epsilon}\right) q^\epsilon$$

dyadic ranges. Referring again to (5-2), the contribution of terms with  $nm \leq q^{1+\epsilon}$  is

$$\leq \frac{5}{2\epsilon} \left(\frac{1}{\epsilon} + 3\right)^{1/4} \max \mathcal{S}_p(N, M) < \frac{3}{\epsilon^{5/4}} \max \mathcal{S}_p(N, M), \quad (5-6)$$

where  $NM < q^{1+\epsilon}$  and  $\mathcal{S}_p(N, M)$  are as in Section 4.

Arguing as in the proof of Lemma 4.1, for every value of  $n$  in  $\mathcal{S}_p$ , there are at most six choices for  $m \bmod p^{k-1}$  and thus the total number of choices for  $m$  is at most  $42(M/q + 1)$ . From this, we get for  $N \leq M$ ,

$$\begin{aligned} \mathcal{S}_p &\leq \frac{42}{(NM)^{1/2}} N \left(\frac{M}{q} + 1\right) \\ &\leq 42 \left( \left(\frac{N}{M}\right)^{1/2} + q^{-1/2+\epsilon} \right) \leq 42 \left( \frac{q^{1/2+\epsilon/2}}{M} + q^{-1/2+\epsilon} \right). \end{aligned} \quad (5-7)$$

As in [Section 4.1](#), the subsum of  $\mathcal{S}_p(N, M)$  consisting of terms with  $p^{k-1} \mid (n^2 - m^2)$  is empty unless  $M \geq q/28$ , in which case their contribution is

$$\leq 42(28q^{-\epsilon/2} + 1)q^{-1/2+\epsilon} < 1200 \cdot q^{-1/2+\epsilon}. \quad (5-8)$$

If  $p = 3$ , this is an upper bound on the full  $\mathcal{S}_3$ .

If  $p = 5$ , we must also consider the terms satisfying  $5^{k-1} \mid (n^2 + m^2)$ . These occur only if  $M \geq q^{1/2}/\sqrt{40}$  and  $n^2 + m^2 = 5^{k-1}h$  for some  $1 \leq h \leq 40M^2/q$ . For each  $h$ , we may bound  $r_q(5^{k-1}h)$  by [\(5-3\)](#) and thus obtain

$$\mathcal{S}_5 \leq 1200 \cdot q^{-1/2+\epsilon} + 120e^{(3/2)e^{2/(5\epsilon)}} \frac{1}{(NM)^{1/2}} \frac{M^2}{q^{1-(5/2)\epsilon}}.$$

If  $M/N < q^{1/3-2\epsilon}$ , then  $M^2/(NM)^{1/2} \leq (M/N)(NM)^{1/2} \leq q^{5/6-(3/2)\epsilon}$  and so

$$\mathcal{S}_5 \leq (1200q^{-1/3} + 3 \cdot 40e^{(3/2)e^{2/(5\epsilon)}})q^{-1/6+\epsilon} \leq 125e^{(3/2)e^{2/(5\epsilon)}} \cdot q^{-1/6+\epsilon}. \quad (5-9)$$

If, on the other hand,  $M/N \geq q^{1/3+2\epsilon}$ , we have  $\mathcal{S}_5 \leq 70 \cdot q^{-1/6+\epsilon}$  by [\(5-7\)](#), so the above holds anyway. The same reasoning for  $p = 7$  yields

$$\mathcal{S}_7 \leq (1200q^{-1/3} + 2 \cdot 3 \cdot 56e^{(3/2)e^{2/(5\epsilon)}})q^{-1/6+\epsilon} \leq 340e^{(3/2)e^{2/(5\epsilon)}} \cdot q^{-1/6+\epsilon}. \quad (5-10)$$

Combining [\(5-4\)](#)–[\(5-6\)](#) and [\(5-8\)](#)–[\(5-10\)](#), we obtain [Theorem 1.1](#) in the effective form

$$\left| \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} |L(\tfrac{1}{2}, \chi)|^2 - \frac{p-1}{p}(\log q + C) \right| \leq c(\epsilon)q^{-\lambda_p+\epsilon}, \quad (5-11)$$

where, for  $0 < \epsilon \leq \lambda_p$ ,

$$c(\epsilon) \leq \frac{3}{2} \log 7 \frac{|\log \epsilon|}{\epsilon} + \frac{1}{\epsilon^3(2\pi e\epsilon)^{1/\epsilon}} + \frac{3,600}{\epsilon^{5/4}} + \frac{1,020}{\epsilon^{5/4}} e^{(3/2)e^{2/(5\epsilon)}} < \frac{1,100}{\epsilon^{5/4}} e^{(3/2)e^{2/(5\epsilon)}}.$$

Indeed, it is seen directly that the function  $f(x) = \frac{3}{2}e^{(2/5)x} - (x + \frac{7}{4}) \log x + 10$  is positive on  $[2, 5]$  and on  $[5, 8]$ , and

$$f'(x) \geq \frac{3}{5}e^{16/5}(x-7) - (\log 8 + \tfrac{1}{8}x - 1) - \frac{39}{32} > 14x - 102 > 0$$

for  $x \geq 8$ , so that  $f(x) > 0$  for all  $x \geq 2$ . Therefore,

$$(2\pi e)^{-1/\epsilon} \epsilon^{-(1/\epsilon+7/4)} < \frac{e^{10}}{(2\pi e)^2} \cdot e^{(3/2)e^{2/(5\epsilon)}} < 76e^{(3/2)e^{2/(5\epsilon)}},$$

which suffices to estimate the second summand; for the others it suffices to note that  $\epsilon^{1/4} |\log \epsilon| \leq 4/e$  and  $e^{(3/2)e^{4/5}} > 28$ .

## Acknowledgements

We would like to thank the referee for constructive suggestions. In particular, the referee suggested that, since our estimates are effective, we demonstrate this aspect of our results by writing down the fully explicit version, and we now do so in the final section of the paper. 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.

## References

- [Blomer and Milićević 2015] V. Blomer and D. Milićević, “The second moment of twisted modular  $L$ -functions”, *Geom. Funct. Anal.* **25**:2 (2015), 453–516. [MR](#) [Zbl](#)
- [Bui 2012] H. M. Bui, “Non-vanishing of Dirichlet  $L$ -functions at the central point”, *Int. J. Number Theory* **8**:8 (2012), 1855–1881. [MR](#) [Zbl](#)
- [Burgess 1963] D. A. Burgess, “On character sums and  $L$ -series, II”, *Proc. London Math. Soc.* (3) **13** (1963), 524–536. [MR](#) [Zbl](#)
- [Chinta 2002] G. Chinta, “Analytic ranks of elliptic curves over cyclotomic fields”, *J. Reine Angew. Math.* **544** (2002), 13–24. [MR](#) [Zbl](#)
- [Conrey and Iwaniec 2000] J. B. Conrey and H. Iwaniec, “The cubic moment of central values of automorphic  $L$ -functions”, *Ann. of Math.* (2) **151**:3 (2000), 1175–1216. [MR](#) [Zbl](#)
- [Davenport 2000] H. Davenport, *Multiplicative number theory*, 3rd ed., Graduate Texts in Mathematics **74**, Springer, 2000. [MR](#) [Zbl](#)
- [Greenberg 1985] R. Greenberg, “On the critical values of Hecke  $L$ -functions for imaginary quadratic fields”, *Invent. Math.* **79**:1 (1985), 79–94. [MR](#) [Zbl](#)
- [Heath-Brown 1981] D. R. Heath-Brown, “The fourth power mean of Dirichlet's  $L$ -functions”, *Analysis* **1**:1 (1981), 25–32. [MR](#) [Zbl](#)
- [Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications **53**, American Mathematical Society, Providence, RI, 2004. [MR](#) [Zbl](#)
- [Katz and Sarnak 1999] N. M. Katz and P. Sarnak, “Zeroes of zeta functions and symmetry”, *Bull. Amer. Math. Soc. (N.S.)* **36**:1 (1999), 1–26. [MR](#) [Zbl](#)
- [Khan and Ngo 2016] R. Khan and H. T. Ngo, “Nonvanishing of Dirichlet  $L$ -functions”, *Algebra Number Theory* **10**:10 (2016), 2081–2091. [MR](#) [Zbl](#)
- [Khan et al. 2016] R. Khan, D. Milićević, and H. T. Ngo, “Non-vanishing of Dirichlet  $L$ -functions in Galois orbits”, *Int. Math. Res. Not.* **2016**:22 (2016), 6955–6978. [MR](#)
- [Milićević 2016] D. Milićević, “Sub-Weyl subconvexity for Dirichlet  $L$ -functions to prime power moduli”, *Compos. Math.* **152**:4 (2016), 825–875. [MR](#)
- [Paley 1931] R. E. A. C. Paley, “On the  $k$ -analogues of some theorems in the theory of the Riemann  $\zeta$ -function”, *Proc. London Math. Soc.* (2) **32**:4 (1931), 273–311. [MR](#) [Zbl](#)
- [Ridout 1958] D. Ridout, “The  $p$ -adic generalization of the Thue–Siegel–Roth theorem”, *Mathematika* **5** (1958), 40–48. [MR](#) [Zbl](#)
- [Rohrlich 1984] D. E. Rohrlich, “On  $L$ -functions of elliptic curves and anticyclotomic towers”, *Invent. Math.* **75**:3 (1984), 383–408. [MR](#) [Zbl](#)



- [Rosen 1984] K. H. Rosen, *Elementary number theory and its applications*, Addison-Wesley, Reading, MA, 1984. [MR](#) [Zbl](#)
- [Soundararajan 2000] K. Soundararajan, “Nonvanishing of quadratic Dirichlet  $L$ -functions at  $s = \frac{1}{2}$ ”, *Ann. of Math. (2)* **152**:2 (2000), 447–488. [MR](#) [Zbl](#)
- [Soundararajan 2007] K. Soundararajan, “The fourth moment of Dirichlet  $L$ -functions”, pp. 239–246 in *Analytic number theory*, edited by W. Duke and Y. Tschinkel, Clay Math. Proc. **7**, Amer. Math. Soc., Providence, RI, 2007. [MR](#) [Zbl](#)
- [Stopple 2003] J. Stopple, *A primer of analytic number theory: from Pythagoras to Riemann*, Cambridge University Press, 2003. [MR](#) [Zbl](#)
- [Young 2011] M. P. Young, “The fourth moment of Dirichlet  $L$ -functions”, *Ann. of Math. (2)* **173**:1 (2011), 1–50. [MR](#) [Zbl](#)
- [Zacharias 2017] R. Zacharias, “Simultaneous non-vanishing for Dirichlet  $L$ -functions”, preprint, 2017. [arXiv](#)

Received: 2017-12-29

Revised: 2018-09-19

Accepted: 2018-10-12

[rrkhan@olemiss.edu](mailto:rrkhan@olemiss.edu)*Department of Mathematics, University of Mississippi,  
University, MS, United States*[rlei@brynmawr.edu](mailto:rlei@brynmawr.edu)*Department of Mathematics, Bryn Mawr College,  
Bryn Mawr, PA, United States*[dmilicevic@brynmawr.edu](mailto:dmilicevic@brynmawr.edu)*Department of Mathematics, Bryn Mawr College,  
Bryn Mawr, PA, United States*

## INVOLVE YOUR STUDENTS IN RESEARCH

*Involve* showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

### MANAGING EDITOR

Kenneth S. Berenhaut Wake Forest University, USA

### BOARD OF EDITORS

Colin Adams	Williams College, USA	Chi-Kwong Li	College of William and Mary, USA
Arthur T. Benjamin	Harvey Mudd College, USA	Robert B. Lund	Clemson University, USA
Martin Bohner	Missouri U of Science and Technology, USA	Gaven J. Martin	Massey University, New Zealand
Nigel Boston	University of Wisconsin, USA	Mary Meyer	Colorado State University, USA
Amarjit S. Budhiraja	U of N Carolina, Chapel Hill, USA	Frank Morgan	Williams College, USA
Pietro Cerone	La Trobe University, Australia	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran
Scott Chapman	Sam Houston State University, USA	Zuhair Nashed	University of Central Florida, USA
Joshua N. Cooper	University of South Carolina, USA	Ken Ono	Emory University, USA
Jem N. Corcoran	University of Colorado, USA	Yuval Peres	Microsoft Research, USA
Toka Diagana	Howard University, USA	Y.-F. S. Pétermann	Université de Genève, Switzerland
Michael Dorff	Brigham Young University, USA	Jonathon Peterson	Purdue University, USA
Sever S. Dragomir	Victoria University, Australia	Robert J. Plemmons	Wake Forest University, USA
Joel Foisy	SUNY Potsdam, USA	Carl B. Pomerance	Dartmouth College, USA
Errin W. Fulp	Wake Forest University, USA	Vadim Ponomarenko	San Diego State University, USA
Joseph Gallian	University of Minnesota Duluth, USA	Bjorn Poonen	UC Berkeley, USA
Stephan R. Garcia	Pomona College, USA	József H. Przytycki	George Washington University, USA
Anant Godbole	East Tennessee State University, USA	Richard Rebarber	University of Nebraska, USA
Ron Gould	Emory University, USA	Robert W. Robinson	University of Georgia, USA
Sat Gupta	U of North Carolina, Greensboro, USA	Javier Rojo	Oregon State University, USA
Jim Haglund	University of Pennsylvania, USA	Filip Saidak	U of North Carolina, Greensboro, USA
Johnny Henderson	Baylor University, USA	Hari Mohan Srivastava	University of Victoria, Canada
Glenn H. Hurlbert	Arizona State University, USA	Andrew J. Sterge	Honorary Editor
Charles R. Johnson	College of William and Mary, USA	Ann Trenk	Wellesley College, USA
K. B. Kulasekera	Clemson University, USA	Ravi Vakil	Stanford University, USA
Gerry Ladas	University of Rhode Island, USA	Antonia Vecchio	Consiglio Nazionale delle Ricerche, Italy
David Larson	Texas A&M University, USA	John C. Wierman	Johns Hopkins University, USA
Suzanne Lenhart	University of Tennessee, USA	Michael E. Zieve	University of Michigan, USA

### PRODUCTION

Silvio Levy, Scientific Editor


Cover: Alex Scorpan

See inside back cover or [msp.org/involve](http://msp.org/involve) for submission instructions. The subscription price for 2019 is US \$195/year for the electronic version, and \$260/year (+\$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2019 Mathematical Sciences Publishers

# involve

2019

vol. 12

no. 3

Darboux calculus	361
MARCO ALDI AND ALEXANDER MCCLEARY	
A countable space with an uncountable fundamental group	381
JEREMY BRAZAS AND LUIS MATOS	
Toeplitz subshifts with trivial centralizers and positive entropy	395
KOSTYA MEDYNETS AND JAMES P. TALISSE	
Associated primes of $h$ -wheels	411
COREY BROOKE, MOLLY HOCH, SABRINA LATO, JANET STRIULI AND BRYAN WANG	
An elliptic curve analogue to the Fermat numbers	427
SKYE BINEGAR, RANDY DOMINICK, MEAGAN KENNEY, JEREMY ROUSE AND ALEX WALSH	
Nilpotent orbits for Borel subgroups of $SO_5(k)$	451
MADELEINE BURKHART AND DAVID VELLA	
Homophonic quotients of linguistic free groups: German, Korean, and Turkish	463
HERBERT GANGL, GIZEM KARAALI AND WOOHYUNG LEE	
Effective moments of Dirichlet $L$ -functions in Galois orbits	475
RIZWANUR KHAN, RUOYUN LEI AND DJORDJE MILIĆEVIĆ	
On the preservation of properties by piecewise affine maps of locally compact groups	491
SERINA CAMUNGOL, MATTHEW MORISON, SKYLAR NICOL AND ROSS STOKKE	
Bin decompositions	503
DANIEL GOTSHALL, PAMELA E. HARRIS, DAWN NELSON, MARIA D. VEGA AND CAMERON VOIGT	
Rigidity of Ulam sets and sequences	521
JOSHUA HINMAN, BORYS KUCA, ALEXANDER SCHLESINGER AND ARSENIY SHEYDVASSER	