MEAN SQUARE OF INVERSES OF DIRICHLET L-FUNCTIONS INVOLVING CONDUCTORS

IU-IONG NG AND YUICHIRO TOMA

Abstract. We deal with negative square moments of Dirichlet L-functions. Summing over characters modulo q, we obtain an asymptotic formula for the negative second moment of $L(1,\chi)$ involving conductors. We also show an application to the analysis of a number theoretic algorithm.

1. Introduction

Let $s=\sigma+it$ be a complex variable. In analytic number theory, special values of Dirichlet L-functions on the real axis have been receiving considerable attention, such as vanishing or non-vanishing at the central point $s=1/2$, and the quantities $L(1,\chi)$ for estimating the class number of cyclotomic fields. Let q be a positive integer and let χ be a Dirichlet character modulo q. The corresponding Dirichlet L-function is defined to be

$$L(s,\chi):=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

for $\sigma>1$, and can be continued analytically over the whole plane, except for the possible pole at $s=1$.

The study of the mean values of Dirichlet L-functions at $s=1$ can be traced back to Paley [21] and Selberg [22] in order to estimate the class number of the cyclotomic field $\mathbb{Q}(\xi_q)$, where ξ_q is a primitive q-th root of unity. They proved in the case of q being a prime number that

$$\sum_{\chi\neq\chi_0}|L(1,\chi)|^2=\zeta(2)q+O\left((\log q)^2\right).$$

The above formula was further studied by Slavutskii [24, 25], Zhang [27], and by Katsurada and Matsumoto [14], who proved the above asymptotic formula with an arbitrarily small error terms. Before their result, a similar formula for $\sigma=1/2$ was proved by Heath-Brown [11]. For more general q, the asymptotic formulas for the $2k$-th power mean value of $|L(1,\chi)|$ were proved by Zhang and Wang [30].

1.1. **Negative moment.** Compared with (positive) mean values, negative mean values of Dirichlet L-functions at $s=1$ have not been much studied. Zhang [28] first studied the $2k$-th negative moments of Dirichlet L-functions at $s=1$. Later, Zhang

2020 *Mathematics Subject Classification.* 11M06, 11R18, 11T71, 68W40.

Key words and phrases. negative moments, Dirichlet L-functions , log-cyclotomic-unit lattice.

and Deng [29] also considered a similar sum. For the family of quadratic Dirichlet L-functions, Granville and Soundararajan [9] obtained asymptotic formulae for negative moments of $L(1,\chi_d)$. Furthermore, in the function field setting, negative moments of quadratic Dirichlet L-functions at $s=1$ were obtained by Lumley [17], and shifted negative moments of quadratic Dirichlet L-functions over function fields were proved by Bui, Florea and Keating [3] and Florea [5]. In addition, Ihara, Murty and Shimura [13] and Matsumoto and Saad Eddin [18] studied the mean value of the $2k$-th power of the logarithmic derivatives of Dirichlet L-functions at $s=1$.

The asymptotic relation for negative moments of the Riemann zeta-function $\zeta(s)$ was considered by Gonek [8], and the following conjecture was proposed.

Conjecture 1.1 (Gonek)**.** *Let $k>0$ be fixed. Then*

$$\frac{1}{T}\int_0^T \left|\zeta\left(\frac{1}{2}+\frac{\delta}{\log T}+it\right)\right|^{-2k} dt \asymp \left(\frac{\log T}{\delta}\right)^{k^2}$$

holds uniformly for $1\le\delta\le\log T$, and

$$\frac{1}{T}\int_0^T \left|\zeta\left(\frac{1}{2}+\frac{\delta}{\log T}+it\right)\right|^{-2k} dt \asymp \begin{cases} (\log T)^{k^2} & k<\frac{1}{2}, \\ (\log\frac{e}{\delta})(\log T)^{k^2} & k=\frac{1}{2}, \\ \delta^{1-2k}(\log T)^{k^2} & k>\frac{1}{2} \end{cases}$$

holds uniformly for $0<\delta\le 1$.

Gonek [8] proved lower bounds which attain the conjectural order of magnitude for $1\le\delta\le\log T$ and all $k>0$, and for $0<\delta\le 1$ for $k<1/2$ assuming the Riemann Hypothesis (RH). Bui and Florea [2] obtained upper bounds in some ranges of δ under the RH. However, for the case $k>3/2$ and $0<\delta\le 1$, the above conjecture seems to contradict with random matrix theory computations due to Berry and Keating [1], Fyodorov and Keating [7], and Forrester and Keating [6]. For more details, see pp.248 in [2].

1.2. **Main results.** In [20], the authors proved an asymptotic formula for

$$\sum_{\chi\neq\chi_0} |L(1,\chi)|^{-2k}, \tag{1.1}$$

where $k\in\mathbb{N}$, assuming the truth of the Generalized Riemann Hypothesis (GRH). After the submission of this paper, the authors were informed that the asymptotic formula (1.1) with prime q can be proved under the weaker assumption of the non-existence of Siegel zeros by using a Lamzouri's result [15, Theorem 9.2].

In contrast, we prove the case $k=1$ for arbitrary natural numbers q, by means of a more standard approach.

Theorem 1.2. *Let q be a positive integer and χ be a Dirichlet character modulo q. Then we have*

$$\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}} \frac{1}{|L(1,\chi)|^2} = \frac{\zeta(2)}{2\zeta(4)} \prod_{p|q}\left(1+\frac{1}{p^2}\right)^{-1} \varphi(q) + O\left(\exp\left(C\frac{\log q}{\log\log q}\right)\right)$$
$$+ \delta_1 \cdot O\left((1-\beta_1)^{-1}\left((\log q)^2 + (1-\beta_1)^{-1}\right)\right) \quad (q\to\infty)$$

for an absolute constant $C>0$, where β_1 denotes the exceptional zero (defined in Proposition 2.1), and $\delta_1 = 1$ if β_1 exists, or $\delta_1 = 0$ otherwise.

From Siegel's theorem (see [19, Corollary 11.15]) which asserts that $1-\beta_1 \geq C(\varepsilon)q^{-\varepsilon}$, we have $(1-\beta_1)^{-1}\left((\log q)^2 + (1-\beta_1)^{-1}\right) \ll_\varepsilon q^\varepsilon$ by resetting ε. Hence the above becomes

$$\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}} \frac{1}{|L(1,\chi)|^2} = \frac{\zeta(2)}{2\zeta(4)} \prod_{p|q}\left(1+\frac{1}{p^2}\right)^{-1} \varphi(q) + O_\varepsilon\left(q^\varepsilon\right). \tag{1.2}$$

Remark 1.3. The difficulty in obtaining the asymptotic behavior of (1.1) for general $k \geq 1$ unconditionally lies in the fact that one needs restrictions on the range of q when estimating sums of generalized divisor functions in arithmetic progressions

$$\sum_{\substack{n\leq x\\ n\equiv a \bmod q}} d_k(n)$$

with $(a,q)=1$. Even applying Shiu's Brun-Titchmarsh estimate [23], if $k\geq 2$ it cannot be shown that the off-diagonal terms in Lemma 2.5 are $O((\log X)^{O_k(1)}/l)$.

We also give the asymptotic formula for the negative square moment twisted by the conductor under the assumption of the nonexistence of the exceptional zero for prime power q.

Theorem 1.4. *Let $q = p^k$ be a power of a prime and χ be a Dirichlet character modulo q. Let d_χ be the conductor of χ. Assuming that the exceptional zero does not exist, then we have*

$$\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}} \frac{1}{d_\chi |L(1,\chi)|^2} = \frac{\zeta(2)}{2\zeta(4)} \frac{(p-1)^2}{p^2+1} k + O\left(\frac{1}{\log p}\right)$$
$$+ O\left(\frac{k^2(\log p)^2(\log k + \log\log p)^2}{p}\right) \quad (p\to\infty)$$

for $k = o\left(\frac{p}{(\log p)^4}\right)$; otherwise for $k \gg p/(\log p)^4$, the above formula implies only the upper bound estimate, i.e.,

$$\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}} \frac{1}{d_\chi |L(1,\chi)|^2} \ll \frac{k^2(\log p)^2(\log k + \log\log p)^2}{p}.$$

If $q = p^k$ is a power of an odd prime p, then there is exactly one quadratic character with conductor p. If $q = 2^k$, then there are at most three primitive quadratic characters with modulus $4, 8$ (see [19, Section 9.3]). Also, by using the lower bounds given by Landau [16], $|L(1,\chi)| \gg 1/\log d_\chi$ for non-quadratic primitive character χ and $|L(1,\chi)| \gg 1/\sqrt{d_\chi}$ for primitive quadratic character χ, and the fact

$$\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}} \frac{1}{d_\chi} \leq \frac{k}{2}$$

(see [4, Claim 3.5]), one can only deduce that

$$\begin{aligned}\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}} \frac{1}{d_\chi\left|L(1,\chi)\right|^2} &= \sum_{\substack{\chi\,:\,\text{non-quadratic}\\ \chi(-1)=1}} \frac{1}{d_\chi\left|L(1,\chi)\right|^2} + O\left(1\right)\\ &\ll k^3(\log p)^2.\end{aligned}$$

Hence, our Theorem 1.4 implies a nontrivial upper bound even for $k \gg \frac{p}{(\log p)^4}$ under the assumption of the nonexistence of the exceptional zero.

Remark 1.5. It is possible to obtain the negative square moment of $L(1,\chi)$ for an odd character χ. By the same argument as in the proof of Theorem 1.2 and Theorem 1.4, we can find that for any integer q,

$$\sum_{\substack{\chi\\ \chi(-1)=-1}} \frac{1}{\left|L(1,\chi)\right|^2} \sim \frac{\zeta(2)}{2\zeta(4)} \prod_{p\mid q}\left(1+\frac{1}{p^2}\right)^{-1} \varphi(q),$$

and for $q = p^k$ with $k = o\left(\frac{p}{(\log p)^4}\right)$ that

$$\sum_{\substack{\chi\\ \chi(-1)=-1}} \frac{1}{d_\chi\left|L(1,\chi)\right|^2} \sim \frac{\zeta(2)}{2\zeta(4)} \frac{(p-1)^2}{p^2+1} k.$$

2. Auxiliary lemmas

In order to obtain Theorem 1.2 and Theorem 1.4, we prove auxiliary lemmas in this section. First, we recall some well-known results from [19].

Proposition 2.1. *Let $q \geq 1$. There is an effectively computable positive constant c_0 such that*

$$\prod_{\chi \bmod q} L(s,\chi)$$

has at most one zero β_1 in the region

$$\sigma \geq 1 - \frac{c_0}{\log q(|t|+1)}.$$

Such a zero, if it exists, is real simple and corresponds to a nonprincipal real character which we denote by χ_1.

Proof. See [19, Theorem 11.3]. □

Proposition 2.2. *Let χ be a nonprincipal character modulo q and suppose that $\sigma > c_0/(2\log q(|t|+1))$. If $L(s,\chi)$ has no exceptional zero , or if β_1 is an exceptional zero of $L(s,\chi)$ but $|s-\beta_1| \geq 1/\log q$, then*

$$\frac{1}{L(s,\chi)} \ll \log q(|t|+1). \tag{2.1}$$

Alternatively, if β_1 is an exceptional zero of $L(s,\chi)$ and $|s-\beta_1| \leq 1/\log q$, then

$$|s-\beta_1| \ll |L(s,\chi)| \ll |s-\beta_1| (\log q)^2. \tag{2.2}$$

Proof. See [19, Theorem 11.4]. □

Lemma 2.3. *Let β_1 be the exceptional zero corresponding to χ_1. Then, the Laurent expansion of the function $1/L(s,\chi_1)$ at the point $s=\beta_1$,*

$$\frac{1}{L(s,\chi_1)} = \sum_{n=-1}^{\infty} P_n (s-\beta_1)^n,$$

satisfies

$$P_n = O\left((\log q)^{n+1}\right). \tag{2.3}$$

Proof. Since β_1 is a simple pole of $1/L(s,\chi_1)$, we have

$$\frac{1}{L(s,\chi_1)} = \sum_{n=-1}^{\infty} P_n (s-\beta_1)^n.$$

For $n \geq 0$, P_n is given by

$$\frac{1}{2\pi i}\int_{\mathcal{C}} \frac{ds}{L(s,\chi_1)(s-\beta_1)^{n+1}}.$$

Here the contour $\mathcal{C}$ is a positively oriented circle of radius $R = c_2/\log(2q)$ and centered at β_1, where $c_2 < c_0/2$ is sufficiently small. By using (2.2), we get

$$P_n \leq \frac{1}{2\pi}\int_0^{2\pi} \frac{R d\theta}{|Re^{i\theta}|\,|Re^{i\theta}|^{n+1}} \leq (\log q)^{n+1}.$$

Otherwise for $n=-1$, we have $P_{-1} = 1/L'(\beta_1,\chi_1)$. Since

$$\frac{1}{L'(s,\chi_1)} = \lim_{s\to\beta_1} \frac{s-\beta_1}{L(s,\chi_1)},$$

by using (2.2) we obtain $P_{-1} \ll 1$. Hence (2.3) is also valid for the case $n=-1$. □

Lemma 2.4 (Character orthogonality)**.** *Let $\mathfrak{a}, \mathfrak{b} \in \{0,1\}$. For n_1, n_2 integers coprime to q, we have*

$$\sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=(-1)^{\mathfrak{a}}}} \frac{\chi(n_1)\overline{\chi}(n_2)}{{d_\chi}^{\mathfrak{b}}}$$

$$= \frac{1}{2} \sum_{\substack{d|q \\ d>1}} \frac{1}{d^{\mathfrak{b}}} \left(\sum_{\substack{l|d \\ n_1 \equiv n_2 \pmod{l}}} \varphi(l)\mu(d/l) + (-1)^{\mathfrak{a}} \sum_{\substack{l|d \\ n_1 \equiv -n_2 \pmod{l}}} \varphi(l)\mu(d/l) \right).$$

The sum on the left-hand side vanishes if $(n_1 n_2, q) \neq 1$.

Proof. This lemma can be proved in a standard way similar to Lemma 1 in [26]. Let $A_{q,d}$ be the set of all Dirichlet characters modulo q whose conductor is d, and B_d be the set of all primitive Dirichlet characters with conductor d. For n_1, n_2 integers coprime to q, it can be rewritten as

$$\sum_{\chi \neq \chi_0} \frac{\chi(n_1)\overline{\chi}(n_2)}{{d_\chi}^{\mathfrak{b}}} = \sum_{\substack{d|q \\ d>1}} \frac{1}{d^{\mathfrak{b}}} \sum_{\chi \in A_{q,d}} \chi(n_1)\overline{\chi}(n_2) = \sum_{\substack{d|q \\ d>1}} \frac{1}{d^{\mathfrak{b}}} \sum_{\chi \in B_d} \chi(n_1)\overline{\chi}(n_2). \tag{2.4}$$

Let $h_{n_1,n_2}(l) := \sum_{\chi \in B_l} \chi(n_1)\overline{\chi}(n_2)$. Since

$$\sum_{l|d} h_{n_1,n_2}(l) = \sum_{\chi \pmod{d}} \chi(n_1)\overline{\chi}(n_2) = \begin{cases} \varphi(d) & n_1 \equiv n_2 \pmod{d}, \\ 0 & \textit{otherwise}, \end{cases}$$

Möbius inversion implies that

$$\sum_{\chi \in B_d} \chi(n_1)\overline{\chi}(n_2) = \sum_{\substack{l|d \\ n_1 \equiv n_2 \pmod{l}}} \varphi(l)\mu(d/l).$$

Hence combining (2.4), we have

$$\sum_{\chi \neq \chi_0} \frac{\chi(n_1)\overline{\chi}(n_2)}{{d_\chi}^{\mathfrak{b}}} = \sum_{\substack{d|q \\ d>1}} \frac{1}{d^{\mathfrak{b}}} \sum_{\substack{l|d \\ n_1 \equiv n_2 \pmod{l}}} \varphi(l)\mu(d/l).$$

Replacing n_2 with $-n_2$, we get the desired result. □

Lemma 2.5. *Let m, n and q be positive integers. For any $l \in \mathbb{N}$ and $X > 1$, we have*

$$\sum_{\substack{m,n=1 \\ (mn,q)=1 \\ m \equiv \pm n \pmod{l}}} \frac{\mu(m)\mu(n)}{mn} e^{-\frac{mn}{X}} = \frac{\zeta(2)}{\zeta(4)} \prod_{p|q} \left(1 + \frac{1}{p^2}\right)^{-1} + O\left(X^{-\frac{1}{2}}\right) + O\left(\frac{(\log X)^2}{l}\right).$$

Proof. First, we calculate the diagonal contribution:

$$\sum_{\substack{m=1 \\ (m,q)=1}}^{\infty} \frac{\mu(m)^2}{m^2} e^{-\frac{m^2}{X}} = \sum_{\substack{m \leq X^{\frac{1}{2}} \\ (m,q)=1}} \frac{\mu(m)^2}{m^2} e^{-\frac{m^2}{X}} + \sum_{\substack{m > X^{\frac{1}{2}} \\ (m,q)=1}} \frac{\mu(m)^2}{m^2} e^{-\frac{m^2}{X}}.$$

If $m > X^{\frac{1}{2}}$, then $e^{-\frac{m^2}{X}} \leq 1$. Therefore, the second sum on the right hand side in the above can be estimated as $X^{-\frac{1}{2}}$. Otherwise, by using $e^{-\frac{m^2}{X}} = 1 + O\left(m^2/X\right)$, we find that the first sum on the right hand side is

$$\sum_{\substack{m=1\\(m,q)=1}}^{\infty} \frac{\mu(m)^2}{m^2} + O\left(X^{-\frac{1}{2}}\right) = \frac{\zeta(2)}{\zeta(4)} \prod_{p|q} \left(1+\frac{1}{p^2}\right)^{-1} + O\left(X^{-\frac{1}{2}}\right). \tag{2.5}$$

By the same manner as in [18], we can calculate the contribution which comes from $m \neq n$ and from $m \equiv n \pmod{l}$. In fact, we have

$$\sum_{\substack{m,n=1\\(mn,q)=1\\m\neq n\\m\equiv n \pmod{l}}}^{\infty} \frac{\mu(m)\mu(n)}{mn} e^{-\frac{mn}{X}} \ll \frac{(\log X)^2}{l}. \tag{2.6}$$

The point different from [18] is that we further treat the nondiagonal terms with $m \neq n$ and $m \equiv -n \pmod{l}$.

$$\begin{aligned}
\sum_{\substack{m,n=1\\(mn,q)=1\\m\neq n\\m\equiv -n \pmod{l}}}^{\infty} \frac{\mu(m)\mu(n)}{mn} e^{-\frac{mn}{X}} &\ll \sum_{\substack{m<n\\(mn,q)=1\\m\equiv -n \pmod{l}}} \frac{e^{-\frac{mn}{X}}}{mn} \\
&= \sum_{m=1}^{\infty} \frac{e^{\frac{m^2}{X}}}{m} \sum_{h>\frac{2m}{l}} \frac{e^{-\frac{mhl}{X}}}{-m+hl} \\
&\ll \frac{1}{l} \sum_{m=1}^{\infty} \frac{e^{\frac{m^2}{X}}}{m} \int_{\frac{2m}{l}}^{\infty} \frac{e^{-\frac{mtl}{X}}}{t-\frac{m}{l}} dt \\
&= \frac{1}{l} \sum_{m=1}^{\infty} \frac{e^{\frac{m^2}{X}}}{m} \left(\int_{\frac{2m}{l}}^{\frac{X}{ml}} + \int_{\frac{X}{ml}}^{\infty}\right) \frac{e^{-\frac{mtl}{X}}}{t-\frac{m}{l}} dt.
\end{aligned}$$

We remark that if $\frac{2m}{l} < \frac{X}{ml}$, then $m \leq \sqrt{\frac{X}{2}}$. Hence the above is equivalent to

$$\frac{1}{l} \sum_{m\leq\sqrt{\frac{X}{2}}} \frac{e^{\frac{m^2}{X}}}{m} \left(\int_{\frac{2m}{l}}^{\frac{X}{ml}} + \int_{\frac{X}{ml}}^{\infty}\right) \frac{e^{-\frac{mtl}{X}}}{t-\frac{m}{l}} dt + \frac{1}{l} \sum_{m>\sqrt{\frac{X}{2}}} \frac{e^{\frac{m^2}{X}}}{m} \int_{\frac{2m}{l}}^{\infty} \frac{e^{-\frac{mtl}{X}}}{t-\frac{m}{l}} dt.$$

Since $t - \frac{m}{l} \geq \frac{m}{l}$ for $t \geq \frac{2m}{l}$, the last term is

$$\begin{aligned}
\frac{1}{l} \sum_{m>\sqrt{\frac{X}{2}}} \frac{e^{\frac{m^2}{X}}}{m} \int_{\frac{2m}{l}}^{\infty} \frac{e^{-\frac{mtl}{X}}}{t-\frac{m}{l}} dt &\ll \sum_{m>\sqrt{\frac{X}{2}}} \frac{e^{\frac{m^2}{X}}}{m^2} \int_{\frac{2m}{l}}^{\infty} e^{-\frac{mtl}{X}} dt \\
&\ll \frac{X}{l} \sum_{m>\sqrt{\frac{X}{2}}} \frac{e^{-\frac{m^2}{X}}}{m^3}
\end{aligned}$$

$$\ll \frac{1}{l}.$$

By using the fact $e^{-mtl/X} \le e^{-2m^2/X}$ for $t \ge \frac{2m}{l}$ and replacing $\frac{mtl}{X} = v$, we have

$$\begin{aligned}
&\frac{1}{l}\sum_{m\le\sqrt{\frac{X}{2}}}\frac{e^{\frac{m^2}{X}}}{m}\left(\int_{\frac{2m}{l}}^{\frac{X}{ml}}+\int_{\frac{X}{ml}}^{\infty}\right)\frac{e^{-\frac{mtl}{X}}}{t-\frac{m}{l}}dt\\
&\ll \frac{1}{l}\sum_{m\le\sqrt{\frac{X}{2}}}\frac{e^{\frac{m^2}{X}}}{m}\int_{\frac{2m}{l}}^{\frac{X}{ml}}\frac{e^{-\frac{2m^2}{X}}}{t-\frac{m}{l}}dt+\frac{1}{l}\sum_{m\le\sqrt{\frac{X}{2}}}\frac{e^{\frac{m^2}{X}}}{m}\int_{1}^{\infty}\frac{e^{-v}}{v-\frac{m^2}{X}}dv\\
&\ll \frac{1}{l}\sum_{m\le\sqrt{\frac{X}{2}}}\frac{e^{-\frac{m^2}{X}}}{m}\int_{\frac{2m}{l}}^{\frac{X}{ml}}\frac{dt}{t-\frac{m}{l}}+\frac{1}{l}\sum_{m\le\sqrt{\frac{X}{2}}}\frac{e^{\frac{m^2}{X}}}{m}\int_{1}^{\infty}\frac{e^{-v}}{v-\frac{1}{2}}dv\\
&\ll \frac{1}{l}\sum_{m\le\sqrt{\frac{X}{2}}}\frac{e^{-\frac{m^2}{X}}}{m}\log\left(\frac{X}{m}+m\right)+\frac{1}{l}\sum_{m\le\sqrt{\frac{X}{2}}}\frac{e^{\frac{m^2}{X}}}{m}\\
&\ll \frac{(\log X)^2}{l}.
\end{aligned}$$

Therefore, we have

$$\sum_{\substack{m,n=1\\(mn,q)=1\\m\ne n\\m\equiv -n \pmod l}}^{\infty}\frac{\mu(m)\mu(n)}{mn}e^{-\frac{mn}{X}} \ll \frac{(\log X)^2}{l}. \tag{2.7}$$

Combining (2.5), (2.6) and (2.7), we obtain the desired result. □

Lemma 2.6. *Let*

$$G_{\mathfrak{b}}(s) := \sum_{\substack{\chi\ne\chi_0\\ \chi(-1)=1}}\frac{1}{d_\chi{}^{\mathfrak{b}}L(s,\chi)L(s,\overline{\chi})},$$

and

$$S_{\mathfrak{b}}(X) := \frac{1}{2\pi i}\int_{3-i\infty}^{3+i\infty}G_{\mathfrak{b}}(s)X^{s-1}\Gamma(s-1)ds. \tag{2.8}$$

Then we have

$$\begin{aligned}
S(X) =&\frac{\zeta(2)}{2\zeta(4)}\prod_{p|q}\left(1+\frac{1}{p^2}\right)^{-1}\sum_{\substack{d|q\\d>1}}\frac{\varphi^*(d)}{d^{\mathfrak{b}}}\\
&+O\left(X^{-\frac{1}{2}}\sum_{\substack{d|q\\d>1}}\frac{1}{d^{\mathfrak{b}}}\sum_{l|d}\varphi(l)\right)+O\left((\log X)^2\sum_{\substack{d|q\\d>1}}\frac{1}{d^{\mathfrak{b}}}\sum_{l|d}\frac{\varphi(l)}{l}\right),
\end{aligned}$$

where $\varphi^*(n)$ denotes the number of primitive characters modulo n.

Proof. By the well-known formula $e^{-y} = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} y^s\Gamma(s)ds$, we have

$$S_{\mathfrak{b}}(X) = \sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}} \frac{1}{d_\chi^{\mathfrak{b}}}\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\frac{\mu(m)\mu(n)\chi(m)\overline{\chi}(n)}{mn}e^{-\frac{mn}{X}}.$$

Now we apply Lemma 2.4 with $\mathfrak{a}=0$, we have

$$S_{\mathfrak{b}}(X) = \frac{1}{2}\sum_{\substack{d|q\\ d>1}}\frac{1}{d^{\mathfrak{b}}}\sum_{l|d}\varphi(l)\mu(d/l)\sum_{\substack{m,n=1\\ (mn,q)=1\\ m=n\\ m\equiv\pm n \pmod l}}^{\infty}\sum_{n=1}^{\infty}\frac{\mu(m)\mu(n)}{mn}e^{-\frac{mn}{X}}.$$

By applying Lemma 2.5, we complete the proof. □

3. Proof of Theorem 1.2

In this section, we prove Theorem 1.2. We assume that q is a positive integer throughout this section. We put $\mathfrak{b}=0$ in Lemma 2.6 to obtain

$$\begin{aligned} S_0(X) &= \frac{\zeta(2)}{2\zeta(4)}\prod_{p|q}\left(1+\frac{1}{p^2}\right)^{-1}\sum_{\substack{d|q\\ d>1}}\varphi^*(d) \\ &\quad + O\left(X^{-\frac{1}{2}}\sum_{\substack{d|q\\ d>1}}\sum_{l|d}\varphi(l)\right) + O\left((\log X)^2\sum_{\substack{d|q\\ d>1}}\sum_{l|d}\frac{\varphi(l)}{l}\right). \end{aligned} \tag{3.1}$$

Now we estimate the integral in (2.8). Put

$$g_\chi(s) := \frac{X^{s-1}\Gamma(s-1)}{L(s,\chi)L(s,\overline{\chi})}.$$

Put $A(c_1) = 1 - c_1/\log(q(T+1))$ with $0 < c_1 < c_0/2$ and shift the part $|t| \le T$ of the path of integration to the line segment $\sigma + it$ defined with $\sigma = A(c_1)$ and $|t| \le T$. Let $\mathcal{C}_T$ denote the closed contour that consists line segments joining the points $3-iT, 3+iT, A(c_1)+iT$ and $A(c_1)-iT$. If there is no exceptional zero, then we take $c_1 = c_0/5$, where c_0 is the constant in Proposition 2.1. If there is an exceptional zero β_1 satisfying $\beta_1 < 1 - c_0/(4\log(q(T+2)))$, then we take $c_1 = c_0/5$ as before. While, if there is an exceptional zero β_1 but $\beta_1 \ge 1 - c_0/(4\log(q(T+2)))$, we take $c_1 = c_0/3$. In the last case, $\mathcal{C}_T$ contains a simple pole at $s=1$ and a pole at $s=\beta_1$ of order 2.

If the exceptional zero β_1 with the associated character χ_1 exists, then putting $u = s-\beta_1$, we write

$$X^{s-1} = X^{\beta_1-1}\sum_{n=0}^{\infty}\frac{(\log X)^n}{n!}u^n$$

and

$$\Gamma(s-1)=\sum_{n=0}^{\infty}\frac{\Gamma^{(n)}(\beta_1-1)}{n!}u^n.$$

Thus, $g_{\chi_1}(s)$ has

$$\begin{aligned}\operatorname{Res}(g_{\chi_1}(s);\beta_1)&=\lim_{s\to\beta_1}\frac{d}{ds}\left[(s-\beta_1)^2\frac{X^{s-1}\Gamma(s-1)}{L(s,\chi_1)^2}\right]\\&=X^{\beta_1-1}\lim_{u\to 0}\frac{d}{du}\left[u^2\frac{X^u\Gamma(u+\beta_1-1)}{L(u+\beta_1,\chi_1)^2}\right]\\&=X^{\beta_1-1}\lim_{u\to 0}\frac{d}{du}\left[\sum_{n=0}^{\infty}R_nu^n\right]\\&=X^{\beta_1-1}R_1,\end{aligned}$$

where

$$R_n=\sum_{\substack{n_1,n_2,n_3\geq 0\\ n=n_1+n_2+n_3}}\left(\sum_{n_1=l_1+l_2}P_{l_1-1}P_{l_2-1}\right)\frac{(\log X)^{n_2}}{n_2!}\frac{\Gamma^{(n_3)}(\beta_1-1)}{n_3!}.$$

Here, P_{l_1-1} and P_{l_2-1} are defined in Lemma 2.3. By using the fact $\Gamma^{(m)}(\beta_1-1)\ll(1-\beta_1)^{-m-1}$, we have

$$\operatorname{Res}(g_{\chi_1}(s);\beta_1)\ll X^{\beta_1-1}(1-\beta_1)^{-1}\left(\log q+\log X+(1-\beta_1)^{-1}\right). \tag{3.2}$$

We apply the residue theorem to obtain

$$\begin{aligned}S_0(X)=&\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}\frac{1}{|L(1,\chi)|^2}+\operatorname{Res}(g_{\chi_1}(s);\beta_1)\\&+\frac{1}{2\pi i}\left(\int_{3+iT}^{A(c_1)+iT}+\int_{A(c_1)+iT}^{A(c_1)-iT}+\int_{A(c_1)-iT}^{3-iT}\right)G_0(s)X^{s-1}\Gamma(s-1)ds\\&+\frac{1}{2\pi i}\int_{\substack{\sigma=3\\|t|>T}}G_0(s)X^{s-1}\Gamma(s-1)ds.\end{aligned}$$

By (2.1) and the Stirling formula (see [19, Theorem C.1])

$$\Gamma(\sigma+it)=\sqrt{2\pi}(1+|t|)^{\sigma-\frac{1}{2}}e^{-\frac{\pi|t|}{2}}(1+O(|t|^{-1})), \tag{3.3}$$

we find from Proposition 2.2 that

$$\begin{aligned}&\frac{1}{2\pi i}\int_{\substack{\sigma=3\\|t|>T}}G_0(s)X^{s-1}\Gamma(s-1)ds\\&\ll\varphi(q)X^2\int_T^{\infty}|\Gamma(2+it)|\,dt\\&\ll\varphi(q)X^2(T+1)^{\frac{3}{2}}e^{-\frac{\pi}{2}T},\end{aligned}$$

$$\begin{aligned}&\frac{1}{2\pi i}\int_{A(c_1)+iT}^{A(c_1)-iT} G_0(s)X^{s-1}\Gamma(s-1)ds\\ &\ll \varphi(q)(\log(q(T+1)))^2 X^{A(c_1)-1}\int_{A(c_1)-iT}^{A(c_1)+iT}|\Gamma(s-1)|\,|ds|\\ &\ll \varphi(q)(\log(q(T+1)))^2 X^{A(c_1)-1},\end{aligned}$$

and

$$\begin{aligned}&\frac{1}{2\pi i}\int_{A(c_1)\pm iT}^{3\pm iT} G_0(s)X^{s-1}\Gamma(s-1)ds\\ &\ll \varphi(q)(\log(q(T+1)))^2 X^{-1}(1+T)^{-\frac{3}{2}}e^{-\frac{\pi T}{2}}\int_{A(c_1)}^{3}((1+T)X)^{\sigma}d\sigma\\ &\ll \varphi(q)(\log(q(T+1)))^2\frac{X^2(1+T)^{\frac{3}{2}}e^{-\frac{\pi T}{2}}}{\log((1+T)X)}.\end{aligned}$$

We now put $T=q$ and $X=\exp\left(\frac{4}{c_0}(\log q)^2\right)$. Then we have

$$\frac{1}{2\pi i}\int_{\substack{\sigma=3\\|t|>T}} G_0(s)X^{s-1}\Gamma(s-1)ds \ll \varphi(q)\exp\left(-\frac{\pi}{2}q\left(1+O\left(\frac{(\log q)^2}{q}\right)\right)\right), \tag{3.4}$$

$$\frac{1}{2\pi i}\int_{A(c_1)+iT}^{A(c_1)-iT} G_0(s)X^{s-1}\Gamma(s-1)ds \ll \frac{\varphi(q)(\log q)^2}{q^2}, \tag{3.5}$$

and

$$\begin{aligned}&\frac{1}{2\pi i}\int_{A(c_1)\pm iT}^{3\pm iT} G_0(s)X^{s-1}\Gamma(s-1)ds\\ &\ll \varphi(q)(\log q)\exp\left(-\frac{\pi}{2}q\left(1+O\left(\frac{\log q)^2}{q}\right)\right)\right).\end{aligned} \tag{3.6}$$

Also from (3.2), we find that the contribution from the exceptional zero is

$$\mathrm{Res}(g_{\chi_1}(s);\beta_1) \ll (1-\beta_1)^{-1}\left((\log q)^2+(1-\beta_1)^{-1}\right).$$

Finally, from the fact $n=\sum_{d|n}\varphi(d)$, we have

$$\begin{aligned}X^{-\frac{1}{2}}\sum_{\substack{d|q\\d>1}}\sum_{l|d}\varphi(l) &\ll \exp\left(-\frac{2}{c_0}(\log q)^2\right)\sum_{\substack{d|q\\d>1}} d\\ &\ll q(\log\log q)\exp\left(-\frac{2}{c_0}(\log q)^2\right).\end{aligned} \tag{3.7}$$

Here we use Gronwall's theorem (see [10, Theorem 323]) in the last step. Similarly, we use $\varphi(n) \le n$ to obtain

$$\begin{aligned}(\log X)^2 \sum_{\substack{d|q \\ d>1}} \sum_{l|d} \frac{\varphi(l)}{l} &\ll (\log q)^4 \sum_{\substack{d|q \\ d>1}} \tau_2(q) \\ &\ll (\log q)^4 \tau_3(q) \\ &\ll (\log q)^4 \exp\left(C \frac{\log q}{\log\log q} \right)\end{aligned}$$

for an absolute constant $C > 0$, where $\tau_k(n) = \sum_{m_1 \dots m_k = n} 1$ denotes the k-fold divisor function. Resetting the constant, we have

$$(\log X)^2 \sum_{\substack{d|q \\ d>1}} \sum_{l|d} \frac{\varphi(l)}{l} \ll \exp\left(C \frac{\log q}{\log\log q} \right). \tag{3.8}$$

Therefore, by combining (3.1), (3.4), (3.5), (3.6), (3.7) and (3.8), we obtain

$$\begin{aligned}\sum_{\substack{\chi \ne \chi_0 \\ \chi(-1)=1}} \frac{1}{|L(1,\chi)|^2} = \frac{\zeta(2)}{2\zeta(4)} \prod_{p|q} \left(1 + \frac{1}{p^2}\right)^{-1} \sum_{\substack{d|q \\ d>1}} \varphi^*(d) + O\left(\exp\left(C \frac{\log q}{\log\log q} \right) \right) \\ + O\left(\delta_1 (1-\beta_1)^{-1} \left((\log q)^2 + (1-\beta_1)^{-1} \right) \right).\end{aligned}$$

Since $\sum_{\substack{d|q \\ d>1}} \varphi^*(d) = \varphi(q) - 1$, we find that the main term in the above is

$$\frac{\zeta(2)}{2\zeta(4)} \prod_{p|q} \left(1 + \frac{1}{p^2}\right)^{-1} \sum_{\substack{d|q \\ d>1}} \varphi^*(d) = \frac{\zeta(2)}{2\zeta(4)} \prod_{p|q} \left(1 + \frac{1}{p^2}\right)^{-1} \varphi(q) + O\left(\exp\left(\omega(q)\right)\right),$$

where $\omega(n)$ denotes the number of distinct prime divisors of n. By using the estimate $\omega(q) \ll \frac{\log q}{\log\log q}$ (see [19, Theorem 2.10]), we complete the proof of Theorem 1.2.

4. Proof of Theorem 1.4

We assume that $q = p^k$ is a prime power and that the exceptional zero does not exist throughout this section. We put $\mathfrak{b} = 1$ in Lemma 2.6 we obtain

$$\begin{aligned}S_1(X) =& \frac{\zeta(2)}{2\zeta(4)} \prod_{p|q} \left(1 + \frac{1}{p^2}\right)^{-1} \sum_{\substack{d|q \\ d>1}} \frac{\varphi^*(d)}{d} \\ &+ O\left(X^{-\frac{1}{2}} \sum_{\substack{d|q \\ d>1}} \frac{1}{d} \sum_{l|d} \varphi(l) \right) + O\left((\log X)^2 \sum_{\substack{d|q \\ d>1}} \frac{1}{d} \sum_{l|d} \frac{\varphi(l)}{l} \right).\end{aligned} \tag{4.1}$$

From the assumption, the function

$$\tilde{g_\chi}(s) := \frac{X^{s-1}\Gamma(s-1)}{d_\chi L(s,\chi) L(s,\overline{\chi})}$$

has only a simple pole at $s = 1$ in the closed contour $\mathcal{C}_T$ which was defined in the previous section. From the residue theorem, we have

$$\begin{aligned}
S_1(X) = & \sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \frac{1}{d_\chi |L(1,\chi)|^2} \\
& + \frac{1}{2\pi i}\left(\int_{3+iT}^{A(c_1)+iT} + \int_{A(c_1)+iT}^{A(c_1)-iT} + \int_{A(c_1)-iT}^{3-iT}\right) G(s)X^{s-1}\Gamma(s-1)ds \\
& + \frac{1}{2\pi i}\int_{\substack{\sigma=3 \\ |t|>T}} G_1(s)X^{s-1}\Gamma(s-1)ds.
\end{aligned}$$

Putting $T = q, X = \exp\left(\frac{6}{c_0}\log q \log\log q\right)$, and by the same argument as in the proof of Theorem 1.2, we find that

$$\begin{aligned}
\frac{1}{2\pi i}\int_{\substack{\sigma=3 \\ |t|>T}} G_1(s)X^{s-1}\Gamma(s-1)ds &\ll \sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \frac{1}{d_\chi}X^2\int_T^\infty |\Gamma(2+it)|\, dt \\
&\ll X^2 q^{\frac{3}{2}} e^{-\frac{\pi}{2}q} \sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \frac{1}{d_\chi} \\
&\ll k\exp\left(-\frac{\pi}{2}q\left(1+O\left(\frac{\log q\log\log q}{q}\right)\right)\right)
\end{aligned} \tag{4.2}$$

since

$$\sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \frac{1}{d_\chi} \leq \frac{k}{2}.$$

By the same argument as above, we have

$$\begin{aligned}
\frac{1}{2\pi i}\int_{A(c_1)+iT}^{A(c_1)-iT} G_1(s)X^{s-1}\Gamma(s-1)ds &\ll \sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \frac{1}{d_\chi}(\log q)^2\exp\left(-\frac{c_0/2}{\log q}\log X\right) \\
&\ll \frac{k}{\log q}
\end{aligned} \tag{4.3}$$

and

$$\begin{aligned}
\int_{A(c_1)\pm iT}^{3\pm iT} G_1(s)X^{s-1}\Gamma(s-1)ds &\ll \sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \frac{1}{d_\chi}(\log q)^2\frac{X^2q^{\frac{3}{2}}e^{-\frac{\pi q}{2}}}{\log(qX)} \\
&\ll k\exp\left(-\frac{\pi}{2}q\left(1+O\left(\frac{\log q\log\log q}{q}\right)\right)\right).
\end{aligned} \tag{4.4}$$

Since $q = p^k$ is a prime power, (4.2), (4.3) and (4.4) can be estimated by

$$\ll \frac{k}{\log q} = \frac{1}{\log p}. \tag{4.5}$$

In order to complete the proof, we estimate the error terms in (4.1). Since $\varphi(n) = n\prod_{p|n}(1-1/p)$, we have

$$(\log X)^2 \sum_{\substack{d>1\\ d|q}} \frac{1}{d} \sum_{l|d} \frac{\varphi(l)}{l} \ll (\log q \log\log q)^2 \sum_{j=1}^{k} \frac{j+1}{p^j}\left(1-\frac{1}{p}\right).$$

We now invoke the generating function for the sum of l-th powers

$$\sum_{l=1}^{\infty} l^n x^l = \frac{x}{(1-x)^{n+1}} A_n(x),$$

where $A_n(x)$ are the Eulerian polynomials that are defined by the exponential generating function

$$\sum_{n=0}^{\infty} A_n(t)\frac{x^n}{n!} = \frac{t-1}{t-e^{(t-1)x}}.$$

By using the fact $A_1(x)=1$ and the definition of X, we have

$$\sum_{j=1}^{k} \frac{j+1}{p^j}\left(1-\frac{1}{p}\right) \ll \sum_{j=1}^{\infty}\frac{j}{p^j} + \sum_{j=1}^{\infty}\frac{1}{p^j} \ll \frac{1}{p}.$$

Hence, we have

$$\begin{aligned}(\log q \log\log q)^2 \sum_{j=1}^{k} \frac{j+1}{p^j}\left(1-\frac{1}{p}\right) &\ll \frac{(\log q \log\log q)^2}{p}\\ &\ll \frac{k^2(\log p)^2(\log k + \log\log p)^2}{p}.\end{aligned}$$

So, we obtain

$$(\log X)^2 \sum_{\substack{d>1\\ d|q}} \frac{1}{d} \sum_{l|d} \frac{\varphi(l)}{l} \ll \frac{k^2(\log p)^2(\log k + \log\log p)^2}{p}. \tag{4.6}$$

Since $n = \sum_{d|n}\varphi(d)$, the second term in (4.1) is

$$X^{-\frac{1}{2}} \sum_{\substack{d>1\\ d|q}} \frac{1}{d} \sum_{l|d} \varphi(l) = k\exp\left(-\frac{3}{c_0}\log q \log\log q\right). \tag{4.7}$$

Finally, since $\varphi^*(p^j) = p^{j-2}(p-1)^2$, the contribution of the first term is

$$\frac{\zeta(2)}{2\zeta(4)}\left(1+\frac{1}{p^2}\right)^{-1} \sum_{\substack{d>1\\ d|q}} \frac{\varphi^*(d)}{d} = \frac{\zeta(2)}{2\zeta(4)}\frac{(p-1)^2}{p^2+1}k. \tag{4.8}$$

Therefore, combining (4.1), (4.5), (4.6), (4.7)and (4.8), we obtain

$$S_1(X) = \frac{\zeta(2)}{2\zeta(4)}\frac{(p-1)^2}{p^2+1}k + O\left(\frac{k^2(\log p)^2(\log k + \log\log p)^2}{p}\right). \tag{4.9}$$

Therefore, we complete the proof of Theorem 1.4.

5. Application in recovering short generators

In this section, we describe an application of our main results to cryptography. We consider the short generator problem, for more details, see [4, 12].

Definition 5.1 (The short generator problem). Let K be a number field with $\mathcal{O}_K$ its ring of integers. Given a generator h of the principal ideal $h\mathcal{O}_K$, the goal of the Short Generator Problem is to recover a generator g of $h\mathcal{O}_K$, i.e., $g\mathcal{O}_K = h\mathcal{O}_K$, satisfying $\|\mathrm{Log}(g)\|_2 = \min_{u\in\mathcal{O}_K^*} \|\mathrm{Log}(h\cdot u)\|_2$. Such a generator g is called a shortest generator of the principal ideal $h\mathcal{O}_K$.

Notice that the notation $\mathrm{Log}(\cdot)$ in the above definition is the logarithmic embedding of the number field defined for a q-th number field K as $\mathrm{Log}(\alpha) = (\log|\sigma_i(\alpha)|)_{i\in G} \in \mathbb{R}^{\varphi(q)/2}$ for all $\alpha \in K$, where σ_j are the complex embeddings and $G \coloneqq \left(\mathbb{Z}_q^*/\{\pm 1\}\right)$. We consider $K = \mathbb{Q}(\zeta_q)$ to be a q-th cyclotomic number field with its group of cyclotomic units $\mathcal{C} = \langle -1, \zeta_q, b_j \mid j \in G\setminus\{1\}\rangle$, where $b_j = \frac{\zeta_q^j - 1}{\zeta_q - 1}$. Let $\mathbf{b}_j \coloneqq \mathrm{Log}(b_j) = \mathrm{Log}(b_{-j})$ for $j \in G\setminus\{1\}$. Then $\{\mathbf{b}_j\}$ forms a basis for $\mathrm{Log}(\mathcal{C})$, the log-cyclotomic-unit lattice of K. We denote by $\{\mathbf{b}_j^\vee\}$ its dual basis corresponding to $\{\mathbf{b}_j\}$.

5.1. Previous results on SGP over cyclotomic number fields.

We combine the implication of Theorem 4.1 of [4] to the special case using the distribution given by Lemma 5.4 of [4], which is the main target of our application, more details and proofs is given in Appendix A.

Theorem 5.2 (implication of [4, Theorem 3.1, Theorem 4.1, Lemma 5.4]). *Let $X_1,\dots, X_{\varphi(q)/2}, X_1',\dots,X_{\varphi(q)/2}'$ be i.i.d. random variables of the Gaussian distribution with the mean 0 and the standard deviation $r>0$, and let $\hat{X}_i = (X_i^2 + X_i'^2)^{1/2}$. Then for any tuple of vectors $\mathbf{v}^{(1)},\dots,\mathbf{v}^{(\varphi(q)/2-1)} \in \mathbb{R}^{\varphi(q)/2}$ of Euclidean norm 1 that are orthogonal to the all-1 vector, and for parameter t such that $\frac{1}{2\|\mathbf{b}_j^\vee\|_2} > t > T$ for some universal constant T,*

$$\Pr\left[\exists j, \left|\sum_i a_i^{(j)} \log(\hat{X}_i)\right| \geq t\right] \leq (\varphi(q)-2)\, e^{-t/2}.$$

Then there is an efficient algorithm that given $g' = g\cdot u$, where g is chosen from the distribution given by $\left(\hat{X}_i\right)$ and u is a cyclotomic unit, outputs an element of the form $\pm\zeta^j g$ with probability at least $1-(\varphi(q)-2)\, e^{(-t/2)}$.

In [4], the relation between the length of the dual basis and the negative square moment of $L(1,\chi)$ is also given. We rephrase the combination of Theorem 3.1 in [4] and the equation given in its proof.

Theorem 5.3 ([4, from the proof of Theorem 3.1]). *Let $q = p^k$ for a prime p, and let $\{\mathbf{b}_j^\vee\}_{j\in G\setminus\{1\}}$ denote the basis dual to $\{\mathbf{b}_j\}_{j\in G\setminus\{1\}}$. Then all $\left\|\mathbf{b}_j^\vee\right\|_2$ are equal, and*

$$\|\mathbf{b}_j^\vee\|_2^2 = 4\,|G|^{-1} \cdot \sum_{\chi\in\hat{G}\setminus\{1\}} d_\chi^{-1} \cdot |L(1,\chi)|^{-2},$$

where $\hat{G}$ is the set of characters of G.

Here we mark out the estimate of the length of the dual basis given by [4].

Theorem 5.4 ([4, part of Theorem 3.1])**.** *Let $q = p^k$ for a prime p, and let $\{\mathbf{b}_j^\vee\}_{j\in G\setminus\{1\}}$ denote the basis dual to $\{\mathbf{b}_j\}_{j\in G\setminus\{1\}}$. Then all $\left\|\mathbf{b}_j^\vee\right\|_2$ are equal, and*

$$\|\mathbf{b}_j^\vee\|_2^2 \le 2k\,|G|^{-1}\cdot\left(\ell(q)^2+O(1)\right) = 4C^2k\frac{(\log q)^2}{q}(1+o(1)),$$

where $\ell(q) = C\log q$ for some $C > 0$.

5.2. **Our improvements.** In this subsection, we show the improvement on estimating the length of the dual basis obtained from applying our main theorems.

If q is a large prime number, then $d_\chi = q$ for all χ modulo q and $\chi \ne \chi_0$. Hence by substituting (1.2) we have

$$\|\mathbf{b}_j^\vee\|_2 = \sqrt{\frac{4\zeta(2)}{\zeta(4)q}\left(1+O\left(q^{-1+\varepsilon}\right)\right)} = \frac{2\sqrt{15}}{\pi\sqrt{q}}\left(1+O\left(q^{-1+\varepsilon}\right)\right).$$

Then there exists $Q > 0$ such that for any $q > Q$,

$$\|\mathbf{b}_j^\vee\|_2 < \frac{2\sqrt{15}}{\pi\sqrt{q}}(1+\delta)$$

for some positive $\delta \ll 1$. Then by applying Theorem 5.2, we obtain the following result.

Corollary 5.5. *Let q be a large prime number. There exists an efficient algorithm that given $g' = g\cdot u$, where g is chosen from $D(t,\alpha)$ and $u \in \mathcal{C}$ is a cyclotomic unit, outputs an element of the form $\pm\zeta^j g$ with probability at least $\alpha = 1-(q-3)e^{-t/2}$ with $t = \frac{\pi}{4\sqrt{15}}\frac{\sqrt{q}}{1+\delta} > T$ for some small $\delta > 0$.*

For the case $q = p^k$ is a prime power, first we assume that $k = o\left(p/(\log p)^4\right)$ with p large enough. Under the assumption of the nonexistence of the exceptional zero, we obtain

$$\begin{aligned}\|\mathbf{b}_j^\vee\|_2 &= \sqrt{\frac{8}{\varphi(p^k)}\left(\frac{\zeta(2)}{2\zeta(4)}\frac{(p-1)^2}{p^2+1}k\left(1+o(1)\right)\right)}\\ &= \frac{2\sqrt{15}}{\pi}\sqrt{\frac{k}{\varphi(p^k)}}\left(1+o(1)\right).\end{aligned}$$

While for the case $k \gg p/(\log p)^4$, under the assumption of the nonexistence of the exceptional zero, we have

$$\|\mathbf{b}_j^\vee\|_2 \ll \frac{k\log p(\log k+\log\log p)}{\sqrt{\varphi(p^k)p}}.$$

Then there exists $Q_1 > 0$ such that for any $q > Q_1$,

$$\begin{aligned}\|\mathbf{b}_j^\vee\|_2 &= \frac{2\sqrt{15}}{\pi}\sqrt{\frac{k}{\varphi(p^k)}}\,(1+o(1))\\ &< \frac{2\sqrt{15}}{\pi}\sqrt{\frac{k}{\varphi(p^k)}}\,(1+\delta_1)\end{aligned}$$

for some positive $\delta_1 \ll 1$. Otherwise, there exists $Q_2 > 0$ such that for any $q > Q_2$,

$$\|\mathbf{b}_j^\vee\|_2 = O\left(\frac{k\log p(\log k + \log\log p)}{\sqrt{\varphi(p^k)p}}\right) \leq C_2\frac{k\log p(\log k + \log\log p)}{\sqrt{\varphi(p^k)p}}$$

for some constant $C_2 > 0$. Thus we derive the following result by applying Theorem 5.2.

Corollary 5.6. *Let $q = p^k$ be a power of a prime number and assume that the exceptional zeros do not exist. There exists an efficient algorithm that given $g' = g \cdot u$, where g is chosen from $D(t,\alpha)$ and $u \in \mathcal{C}$ is a cyclotomic unit, outputs an element of the form $\pm\zeta^j g$ with probability at least $\alpha = 1 - (\varphi(q) - 2)e^{-t/2}$ with $t = \frac{\pi}{4\sqrt{15}}\sqrt{\frac{\varphi(q)}{k}}\frac{1}{1+\delta} > T$ for some small $\delta > 0$ if $k = o\left(\frac{p}{(\log p)^4}\right)$ and $T < t \leq \frac{\sqrt{\varphi(q)p}}{2\log q\log\log q}$ otherwise.*

We list the estimates on the length of the dual basis and the corresponding lower bounds on the success probability of the algorithm described in Theorem 5.2, in terms of t, in Table 1. One can observe that when q is a prime number, we improve t by a log term and also get the optimal description of order of t for Theorem 5.2's setting other than only a lower bound. Notice that compared to the prior work [20], we remove the GRH assumption. For prime power q, the bound for $L(1,\chi)$ doesn't change, so that [4] has the same estimate for the dual basis. Therefore, we improve the estimate under assuming the exceptional zeros don't exist for both cases, $k = o\left(p/(\log p)^4\right)$ with large prime p ("first q^k condition" henceforth), and $k \gg p/(\log p)^4$. Moreover, since the estimates on the dual basis for prime q and for the first q^k condition are equalities, their parameters t and the corresponding lower bound on the success probability are optimal for Theorem 5.2's setting.

TABLE 1. Comparison: the constant C refer to the one in Theorem 5.4.

Condition and approach	$\left\lVert \mathbf{b}_j^\vee \right\rVert_2$	Parameter t in Theorem 5.2
$q = p^k$; bound on $L(1, \chi)$ [4]	$\leq 2C\sqrt{k}\frac{\log q}{\sqrt{q}}(1 + o(1))$	$\gg \frac{\sqrt{q}}{\sqrt{k}\log q}$
q: large prime; negative moment	$= \frac{2\sqrt{15}}{\pi\sqrt{q}}\left(1 + O\left(q^{-1+\varepsilon}\right)\right)$	$\asymp \sqrt{q}$
$q = p^k$ with p: large prime, $k = o\left(p/(\log p)^4\right)$; negative moment (assuming the nonexistence of exceptional zeros)	$= \frac{2\sqrt{15}}{\pi}\sqrt{\frac{k}{\varphi(q)}}\,(1 + o(1))$	$\asymp \sqrt{\frac{q}{k}}$
$q = p^k$ with p: prime, $k \gg p/(\log p)^4$; negative moment (assuming the nonexistence of exceptional zeros)	$\ll \frac{\log q \log\log q}{\sqrt{\varphi(q)p}}$	$\gg \frac{\sqrt{qp}}{\log q \log\log q}$

Acknowledgements. The authors would like to thank Professor Kohji Matsumoto for reading the manuscript carefully and giving them valuable comments. The authors would also like to thank Professor François Le Gall for his financial support. The authors would also like to thank Professor Nathan Ng for informing them Lamzouri's result. I.-I. Ng is supported by MEXT Q-LEAP grant No. JPMXS0120319794. Y. Toma is supported by Grant-in-Aid for JSPS Research Fellow grant No. 24KJ1235.

REFERENCES

[1] M. V. Berry and J. P. Keating. "Clusters of near-degenerate levels dominate negative moments of spectral determinants". *J. Phys. A* 35.1 (2002), pp. L1–L6.
[2] H. M. Bui and A. Florea. "Negative moments of the Riemann zeta-function". *J. Reine Angew. Math.* 806 (2024), pp. 247–288.
[3] H. M. Bui, A. Florea, and J. P. Keating. "The ratios conjecture and upper bounds for negative moments of L-functions over function fields". *Trans. Amer. Math. Soc.* 376.6 (2023), pp. 4453–4510.
[4] R. Cramer, L. Ducas, C. Peikert, and O. Regev. "Recovering short generators of principal ideals in cyclotomic rings". *Advances in cryptology—EUROCRYPT 2016. Part II*. Vol. 9666. Lecture Notes in Comput. Sci. 2016, pp. 559–585.
[5] A. Florea. "Negative moments of L-functions with small shifts over function fields". *Int. Math. Res. Not. IMRN* 3 (2024), pp. 2298–2337.

[6] P. J. Forrester and J. P. Keating. “Singularity dominated strong fluctuations for some random matrix averages”. *Comm. Math. Phys.* 250.1 (2004), pp. 119–131.

[7] Y. V. Fyodorov and J. P. Keating. “Negative moments of characteristic polynomials of random GOE matrices and singularity-dominated strong fluctuations”. *J. Phys. A* 36.14 (2003), pp. 4035–4046.

[8] S. M. Gonek. “On negative moments of the Riemann zeta-function”. *Mathematika* 36.1 (1989), pp. 71–88.

[9] A. Granville and K. Soundararajan. “The distribution of values of $L(1, \chi_d)$”. *Geom. Funct. Anal.* 13.5 (2003), pp. 992–1028.

[10] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers.* Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

[11] D. R. Heath-Brown. “An asymptotic series for the mean value of Dirichlet L-functions”. *Comment. Math. Helv.* 56.1 (1981), pp. 148–161.

[12] P. Holzer, T. Wunderer, and J. A. Buchmann. “Recovering short generators of principal fractional ideals in cyclotomic fields of conductor $p^\alpha q^\beta$”. *Progress in cryptology—INDOCRYPT 2017.* Vol. 10698. Lecture Notes in Comput. Sci. 2017, pp. 346–368.

[13] Y. Ihara, V. K. Murty, and M. Shimura. “On the logarithmic derivatives of Dirichlet L-functions at $s = 1$”. *Acta Arith.* 137.3 (2009), pp. 253–276.

[14] M. Katsurada and K. Matsumoto. “The mean values of Dirichlet L-functions at integer points and class numbers of cyclotomic fields”. *Nagoya Math. J.* 134 (1994), pp. 151–172.

[15] Y. Lamzouri. “The two-dimensional distribution of values of $\zeta(1+it)$”. *Int. Math. Res. Not. IMRN* (2008), Art. ID rnn 106, 48.

[16] E. Landau. “Über Dirichletsche Reihen mit komplexen Charakteren”. *J. Reine Angew. Math.* 157 (1927), pp. 26–32.

[17] A. Lumley. “Complex moments and the distribution of values of $L(1, \chi_D)$ over function fields with applications to class numbers”. *Mathematika* 65.2 (2019), pp. 236–271.

[18] K. Matsumoto and S. Saad Eddin. “An asymptotic formula for the $2k$-th power mean value of $|(L'/L)(1+it_0, \chi)|$”. *J. Math. Soc. Japan* 73.3 (2021), pp. 781–814.

[19] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory.* Vol. 97. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2007.

[20] I.-I. Ng and Y. Toma. “Recovering short generators via negative moments of Dirichlet L-functions”. *arXiv preprint: 2405.13420* (2024).

[21] R. E. A. C. Paley. “On the k-Analogues of some Theorems in the Theory of the Riemann ζ-Function”. *Proc. London Math. Soc. (2)* 32.4 (1931), pp. 273–311.

[22] A. Selberg. “Contributions to the theory of Dirichlet’s L-functions”. *Skr. Norske Vid.-Akad. Oslo I* 1946.3 (1946), p. 62.

[23] P. Shiu. “A Brun-Titchmarsh theorem for multiplicative functions”. *J. Reine Angew. Math.* 313 (1980), pp. 161–170.

[24] I. S. Slavutskii. "Mean value of L-functions and the class number of a cyclotomic field". *Algebraic systems with one action and relation*. Leningrad. Gos. Ped. Inst., Leningrad, 1985, pp. 122–129.

[25] I. S. Slavutskii. "Mean value of L-functions and the class number of a cyclotomic field". *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* 154 (1986), pp. 136–143, 178–179.

[26] K. Soundararajan. "The fourth moment of Dirichlet L-functions". *Analytic number theory*. Vol. 7. Clay Math. Proc. Amer. Math. Soc., Providence, RI, 2007, pp. 239–246.

[27] W. Zhang. "On the mean value of the L-function". *J. Math. Res. Exposition* 10.3 (1990), pp. 355–360.

[28] W. Zhang. "The $2k$th power means of inverses of Dirichlet L-functions". *Chinese Ann. Math. Ser. A* 14.1 (1993), pp. 1–5.

[29] W. Zhang and Y. Deng. "A hybrid mean value of the inversion of L-functions and general quadratic Gauss sums". *Nagoya Math. J.* 167 (2002), pp. 1–15.

[30] W. Zhang and W. Wang. "An exact calculating formula for the $2k$-th power mean of L-functions". *JP J. Algebra Number Theory Appl.* 2.2 (2002), pp. 195–203.

Appendix A. Proof Theorem 5.2

In this section, we describe the details and the proof of Theorem 5.2. As in [4], we assume that the index $[\mathrm{Log}(\mathcal{O}_K^*) : \mathrm{Log}(\mathcal{C})]$ is small.

We denote by $D(t, \alpha)$ the distribution over K with the property that for any tuple of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_\ell \in \mathbb{R}^{\varphi(q)/2}$ of Euclidean norm 1 that are orthogonal to the all-1 vector $\mathbf{1}$, the probability that $|\langle \mathrm{Log}(g), \mathbf{v}_j \rangle| < t$ holds for all $j = 1, \ldots, \ell$ is at least some $\alpha > 0$, where g is chosen from $D(t, \alpha)$ and the parameter t is positive (remembering that $\mathrm{Log}(K) \subset \mathbb{R}^{\varphi(q)/2}$).

The following is an immediate result from the fact that the image $\mathrm{Log}(u) \in \mathbb{R}^{\varphi(q)/2}$ for $u \in \mathcal{O}_K^*$ is orthogonal to the all-1 vector.

Lemma A.1. *Let g be chosen from $D(t, \alpha)$. Then $\left| \left\langle \mathrm{Log}(g), \frac{\mathbf{b}_j^\vee}{\|\mathbf{b}_j^\vee\|_2} \right\rangle \right| < t$ holds for all $j = 1, \ldots, \varphi(q)/2$ with probability at least α.*

Below, we specify the parameters in our setting of K for some certain Gaussian distributions.

Lemma A.2. *Let $n = \varphi(q)/2$ and $\ell = n - 1$. Then $D(t, \alpha)$ with $t > 0$ and $\alpha = 1 - (\varphi(q) - 2)e^{-t/2}$ exists for some Gaussian distributions that have standard deviation r if $t \geq T$, where T is the universal constant given in [4, Lemma 5.4].*

Proof of Lemma A.2. The corollary follows immediately from [4, Lemma 5.4] over K by taking $n = \varphi(q)/2$ and $\ell = n - 1$. Here we identify the elements of K by real and imaginary parts of their image under complex embeddings, i.e., $\Psi : \mathcal{O}_K \to \mathbb{R}^{\varphi(q)}$ such that $\Psi(a) = (\mathrm{Re}(\sigma_j(a)), \mathrm{Im}(\sigma_j(a)))_{j=1,\ldots,\varphi(q)/2}$. More precisely, the random variables X_i and X_i' correspond to $(\mathrm{Re}(\sigma_i(a)))_{a \in K}$ and $(\mathrm{Im}(\sigma_i(a)))_{a \in K}$, respectively. It follows that the random variables $\hat{X}_i$ correspond to $(|\sigma_i(a)|)_{a \in K}$ and thus $\log\left(\hat{X}_i\right)$ correspond to

$(\mathrm{Log}(a))_{a\in K}$. Let $\mathbf{v}^{(1)},\ldots,\mathbf{v}^{(\varphi(q)/2-1)}\in\mathbb{R}^{\varphi(q)/2}$ be vectors with Euclidean norm 1 that are orthogonal to the all-1 vector. Therefore, [4, Lemma 5.4] indicates that for entries $v_i^{(j)}$ of $\mathbf{v}^{(j)}$,

$$\Pr\left[\exists j,\left|\sum_i v_i^{(j)}\log(\hat{X}_i)\right|\geq t\right]\leq(\varphi(q)-2)\,e^{-t/2},$$

which implies that

$$\Pr\left[\left|\left\langle\left(\mathrm{Log}(\hat{X}_i)\right)_{i=1,\ldots,\varphi(q)/2},\mathbf{v}^{(j)}\right\rangle\right|<t\text{ for all }j=1,\ldots,\varphi(q)/2-1\right]$$
$$>1-(\varphi(q)-2)\,e^{-t/2}.$$

Hence, $\hat{X}_1,\ldots,\hat{X}_{\varphi(q)/2}$ are i.i.d. $D\left(t,1-(\varphi(q)-2)\,e^{-t/2}\right)$ random variables. □

We first show an immediate consequence deduced from results of [4].

Corollary A.3. *If the parameter t satisfies $\frac{1}{2\left\|\mathbf{b}_j^\vee\right\|_2}>t>T$ for some universal constant T, then there is an efficient algorithm that given $g'=g\cdot u$, where g is chosen from the distribution given by $D(t,\alpha)=D(t,1-(\varphi(q)-2)\,e^{-t/2})$ and $u\in\mathcal{C}$ is a cyclotomic unit, outputs an element of the form $\pm\zeta^j g$ with probability at least $\alpha=1-(\varphi(q)-2)\,e^{-t/2}$.*

We mainly follow the proof of [4, Theorem 4.1], and take care of the parameters and probability.

Proof. Let t satisfies that $\frac{1}{2\left\|\mathbf{b}_j^\vee\right\|_2}>t>T$. The idea is to find the magnitude of u by computing $\mathrm{Log}(u)$, and to divide g' by u. Notice that under the logarithmic embedding, we have the relation $\mathrm{Log}(g')=\mathrm{Log}(g)+\mathrm{Log}(u)\in\mathbb{R}^{\varphi(q)/2}$ with $\mathrm{Log}(u)\in\mathrm{Log}(\mathcal{C})$ and $\mathrm{Log}(g)\in\mathrm{Log}(\mathcal{O}_K^*)$, whose form is suitable for Babai's round-off algorithm ([4, Claim 2.1]).

Then the algorithm goes by first finding $\mathrm{Log}(u)$ with Babai's algorithm, then computing $u'=\prod b_j^{a_j}$, where a_j are integer coefficients of $\mathrm{Log}(u)=\sum a_j\mathbf{b}_j$, and finally outputting g'/u'. Since $\mathrm{Log}(u')=\mathrm{Log}(u)$ implies that $g'/u'=gu/u'=\pm\zeta^j g$ for some sign and some $j\in\{1,\ldots,q\}$, it suffices to show the fitness for applying Babai's algorithm, and the probability for allowing to apply it.

From Theorem 5.3, the short generator algorithm succeeds only if Babai's algorithm succeeds. According to [4, Claim 2.1], in order to apply Babai's algorithm, we need to ensure the input generator g meets the requirement that

$$\left|\langle\mathrm{Log}(g),\mathbf{b}_j^\vee\rangle\right|<1/2$$

for all $j\in G\setminus\{1\}$.

By Lemma A.1 and the assumption $\frac{1}{2\|\mathbf{b}_j^\vee\|_2} > t$, we have

$$\begin{aligned}\left|\langle \mathrm{Log}(g), \mathbf{b}_j^\vee \rangle\right| &= \|\mathbf{b}_j^\vee\|_2 \cdot \left|\left\langle \mathrm{Log}(g), \frac{\mathbf{b}_j^\vee}{\|\mathbf{b}_j^\vee\|_2} \right\rangle\right| \\ &< \|\mathbf{b}_j^\vee\|_2 \cdot t \\ &< \frac{1}{2}\end{aligned}$$

as claimed. Then by Lemma A.2 and the assumption that $t \geq T$, the success probability is lower bounded by $\alpha = 1 - (\varphi(q) - 2)e^{-t/2}$ as claimed. □

Then Theorem 5.2 immediately follows [4, Theorem 3.1, Theorem 4.1, Lemma 5.4] and Corollary A.3.

(Ng) Graduate School of Mathematics, Nagoya University, Japan.
Current address: Waseda Research Institute for Science and Engineering, Waseda University, 17 Kikui-cho, Shinjuku-ku, Tokyo 162-0044, Japan.
Email address: `iuiongng@aoni.waseda.jp`

(Toma) Graduate School of Mathematics, Nagoya University, Furo-cho, Chikusa-ku, Nagoya 464-8602, Japan.
Current address: Global Education Center, Waseda University, 1-6-1 Nishiwaseda, Shinjuku-ku, Tokyo 169-8050, Japan.
Email address: `yuichiro.toma@aoni.waseda.jp`