DISS. ETH NO. 23624

Algebraic Twists of Modular Forms and Sums over Primes to Squarefree Moduli

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES of ETH ZURICH

(Dr. sc. ETH Zurich)

presented by

Benny Löffel

MSc ETH Mathematik

born on 10.07.1987
citizen of Worben BE

accepted on the recommendation of

Prof. Dr. Emmanuel Kowalski, examiner
Prof. Dr. Étienne Fouvry, co-examiner

2016

Abstract

In this thesis, we consider the question of whether Fourier coefficients of modular forms correlate with functions of algebraic origin. For a big class of cusp forms f, we show that there is no correlation with many algebraic functions often encountered in number theory. This question was studied before by É. Fouvry, E. Kowalski und Ph. Michel in [22] and our results are a generalisation of the ones in [22].

For a squarefree number q, we consider the correlation sums

$$\mathcal{S}(f, K; q) = \sum_{n<Pq} \rho_f(n) K(n),$$

also called "algebraic twists", where the $\rho_f(n)$'s denote the Fourier coefficients of the cusp form f, $P > 0$ is a parameter and K denotes a function of algebraic origin defined modulo q. Examples of such functions K for which we can prove the non-correlation include Dirichlet characters to the modulus q, $K(n) = \chi(n)$, as well as Hyper-Kloosterman sums

$$K(n) = \mathrm{Kl}_m(n; q) = q^{-\frac{m-1}{2}} \sum_{\substack{x_1,\ldots,x_m \in (\mathbb{Z}/q\mathbb{Z})^\times \\ x_1 \cdots x_m = n}} e\left(\frac{x_1 + \cdots + x_m}{q}\right).$$

These functions share the property that they can be written as a product of trace functions and we show in general that for every such product K,

$$\mathcal{S}(f, K; q) \ll_{f,\delta,P,\mathrm{cond}(K)} q^{1-\delta}$$

for all $\delta < \frac{1}{16}$, where $\mathrm{cond}(K)$ denotes the conductor of K.

As an application, we consider sums over primes and show the upper bound

$$\sum_{\substack{p<Pq \\ p \text{ prime}}} K(p) \ll_P q^{1-\frac{\eta}{2}}$$

for all $\eta < \frac{1}{24}$, K as above.

Zusammenfassung

In dieser Arbeit gehen wir der Frage nach, wann Fourierkoeffizienten von Modulformen mit Funktionen algebraischen Ursprungs korrelieren. Wir zeigen für eine grosse Klasse von Spitzenformen f, dass viele in der Zahlentheorie verwendete Funktionen nicht mit den Fourierkoeffizienten von f korrelieren. Diese Frage wurde zuvor bereits von É. Fouvry, E. Kowalski und Ph. Michel in [22] untersucht und unsere Ergebnisse stellen eine Verallgemeinerung der in [22] enthaltenen Resultate dar.

Konkret betrachten wir für eine quadratfreie Zahl q die Korrelationssummen

$$\mathcal{S}(f,K;q) = \sum_{n<Pq} \rho_f(n)K(n),$$

welche auch als "algebraische Verdrehungen" ("algebraic twists" auf Englisch) bezeichnet werden. Dabei bezeichnen die $\rho_f(n)$'s die Fourierkoeffizienten der Spitzenform f, $P > 0$ ist ein Parameter und K ist eine Funktion algebraischen Ursprungs, welche modulo q definiert ist. Beispiele solcher Funktionen K, für welche wir die Nicht-Korrelation zeigen können, sind Dirichlet-Charaktere zum Modulus q, $K(n) = \chi(n)$ oder Hyper-Kloostermansummen

$$K(n) = \mathrm{Kl}_m(n;q) = q^{-\frac{m-1}{2}} \sum_{\substack{x_1,\dots,x_m \in (\mathbb{Z}/q\mathbb{Z})^\times \\ x_1\cdots x_m = n}} e\left(\frac{x_1+\cdots+x_m}{q}\right).$$

Diesen Funktionen ist gemeinsam, dass sie als Produkt von Spurfunktionen geschrieben werden können. Wir zeigen allgemein für alle solche Produkte von Spurfunktionen K, dass

$$\mathcal{S}(f,K;q) \ll_{f,\delta,P,\mathrm{cond}(K)} q^{1-\delta}$$

für alle $\delta < \frac{1}{16}$ gilt, wobei $\mathrm{cond}(K)$ den Führer von K bezeichnet.

Als Anwendung davon betrachten wir Summen über Primzahlen und beweisen die obere Schranke

$$\sum_{\substack{p<Pq \\ p \text{ prime}}} K(p) \ll_P q^{1-\frac{\eta}{2}}$$

für $\eta < \frac{1}{24}$ und für gewisse Funktionen K algebraischen Ursprungs, welche modulo q definiert sind. Für $K(n) = \mathrm{Kl}_2(na,q)$ stellt dies in gewissen Fällen eine Verbesserung eines Ergebnisses (Lemma 6.1 in [16]) von H. Iwaniec, W. Luo und P. Sarnak dar.

Table of Contents

List of Symbols and Notations

1. Introduction

Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of complex numbers and consider the sum

$$S(x) = \sum_{\substack{n\in\mathbb{N}\\ n<x}} a_n. \tag{1.1}$$

Such sums are ubiquitous in analytic number theory and very often, if the sequence $(a_n)_{n\in\mathbb{N}}$ is bounded and "random enough", one hopes for some cancellation, i.e., one expects that the sum is relatively small compared to x. By heuristic arguments based on the central limit theorem, the best one normally can hope for is squareroot cancellation, i.e., that $S(x) \ll \sqrt{x}$. A famous example is $a_n = \mu(n)$ the Möbius function, where one can show that

$$\sum_{n<x} \mu(n) \ll_\varepsilon x^{\frac{1}{2}+\varepsilon}$$

for every $\varepsilon > 0$, is equivalent to the Riemann hypothesis. The best known bound is

$$\sum_{n<x} \mu(n) \ll x \exp\Big(- c(\log x)^{\frac{3}{5}} (\log\log x)^{-\frac{1}{5}}\Big),$$

coming from the analogous (best known) bound in the prime number theorem [17, p. 227 and p. 124]. This example already illustrates, that even though one expects very often squareroot cancellation, what one actually can prove is much less. Even though the bounds we can prove are far from what is conjectured to be true, they are still sufficient for many applications.

A slightly more general setting often encountered is the case where one has two bounded sequences of complex numbers $(b_n)_{n\in\mathbb{N}}$ and $(c_n)_{n\in\mathbb{N}}$ and one is interested in the twisted sum or "inner product"

$$\sum_{\substack{n\in\mathbb{N}\\ n<x}} b_n\overline{c_n}.$$

If the sequences b_n and c_n do not "correlate", one expects that the sequence $(b_n\overline{c_n})_{n\in\mathbb{N}}$ behaves "randomly" and hence the twisted sum should be small due to cancellation. On the other hand, if the sequences "correlate", such a cancellation can not be expected. As an example, consider $b_n = c_n = \mu(n)$. In this case, the sum

$$\sum_{\substack{n\in\mathbb{N}\\ n<x}} b_n\overline{c_n} = \sum_{\substack{n\in\mathbb{N}\\ n<x}} \mu(n)^2 = \sum_{\substack{n<x\\ n \text{ squarefree}}} 1 = \frac{6}{\pi^2}x + O\big(\sqrt{x}\big)$$

is large. The idea is now, that if the sequence $(b_n)_{n\in\mathbb{N}}$ comes from "a certain world", as for example the Möbius function μ comes from the arithmetic world, and the other sequence $(c_n)_{n\in\mathbb{N}}$ comes from "another world", as for example the automorphic world where the Fourier coefficients of modular forms reside, then the two sequences should not correlate and the twisted sum should be small. Heuristically, one argues that the sequence $(\overline{c_n})_{n\in\mathbb{N}}$ is too different to be able to correlate with the sequence $(b_n)_{n\in\mathbb{N}}$ and hence the resulting twisted sequence $(b_n\overline{c_n})_{n\in\mathbb{N}}$ should behave randomly, which should imply cancellation.

In this thesis, we will consider twisted sums, where the intricate algebraic information is given by Fourier coefficients of modular forms. Modular forms are well used in number theory as well as other parts of mathematics. One reason why they are so useful is, that there are many modular forms whose Fourier coefficients contain useful arithmetic information. Many nice examples can be found in part one of Zagier's article in "The 1-2-3 of Modular Forms", see [4]. An application is given by Fouvry, Kowalski and Michel in [23, p. 1695], where one uses that the twisted divisor function

$$d_u(n) = \sum_{ab=n} \left(\frac{a}{b}\right)^u$$

is (up to normalization) the Fourier coefficient of the nonholomorphic Eisenstein series

$$E(z,s) = \frac{1}{2} \sum_{(c,d)=1} \frac{y^s}{|cz+d|^{2s}},$$

for $s = \frac{1}{2} + it$.

Therefore we may ask in general, whether a bounded sequence $K(n)$ correlates with the sequence $(\rho_f(n))_{n\geq 1}$ of Fourier coefficients of some modular form f. To make this precise, we say that $(K(n))_{n\geq 1}$ does not correlate with the Fourier coefficients of f if we have

$$\sum_{n\leq x} \rho_f(n)K(n) \ll_A x(\log x)^{-A}$$

for all $A \geq 1$. As explained before, heuristically, one expects that a function K does not correlate if it is of "algebraic nature" and not too complex. A special class of such functions K which do not correlate are trace functions with small conductor as introduced in Section 2.3. In this thesis, we will actually consider a slightly more general class of functions K, which we call (q, M)-good (see Definition 2.2.7). Concretely, we will consider sums of the form

$$\sum_{n\leq x} \rho_f(n)K(n)$$

or more precisely smoothed versions thereof

$$\sum_{n\geq 1} \rho_f(n)K(n)V\left(\frac{n}{q}\right),$$

where V is a smooth compactly supported function on $]0, +\infty[$. Such sums were already extensively studied by Fouvry, Kowalski and Michel in [22] and [23] for trace functions $K\colon \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{C}$, with p prime. For example, they show the non-trivial bound

$$\sum_{n\in I} \rho_f(n)K(n) \ll p^{1-\delta}$$

for any interval $I \subset [1,p]$ and any $\delta < \frac{1}{16}$, where the implied constant depends only on f, δ and the conductor of K. In this thesis, we will consider the more general case where the function K is given by

$$K(n) = \prod_{p|q} K_p(n),$$

where q is a squarefree integer and $K_p\colon \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{C}$ are suitable functions, i.e., trace functions with small conductor.

As an example of such a function K, consider the normalized hyper-Kloosterman sum in $m-1$ variables given by

$$\mathrm{Kl}_m(a;q) = q^{-\frac{m-1}{2}} \sum_{\substack{x_1,\dots,x_m \in (\mathbb{Z}/q\mathbb{Z})^\times \\ x_1\cdots x_m = a}} e\left(\frac{x_1+\cdots+x_m}{q}\right)$$

for $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ and some squarefree modulus q. As is shown in [22, Section 10.3], such hyper-Kloosterman sums are functions of the type described above. As we will see later, an application is the bound for a sum over primes

$$\sum_{\substack{p<X \\ p \text{ prime}}} \mathrm{Kl}_2(np;q)\log p \ll_\eta X\Big(1+\frac{q}{X}\Big)^{\frac{1}{12}} q^{-\eta} \tag{1.2}$$

for ever $0 < \eta < \frac{1}{48}$, every $X \geq 2$ and every integer n coprime with q. This bound is a generalisation of [23, Corollary 1.13] to squarefree modulus and an improvement of Luo, Iwaniec and Sarnak's result [16, Lemma 6.1] for $c = q$ squarefree and $X \leq q$. We will present some other examples of trace functions in Section 7.

More simple examples of trace functions include $K(n) = e(an/q)$ an additive character modulo q and $K(n) = \chi(n)$, where χ is a Dirichlet character modulo q as in Example 2.3.4. As explained in [22, Section 1.1], these special cases have been studied already much earlier by several people, see e.g. [15, Theorem 5.3] and [14, Theorem 8.1] for K an additive character and [10], [5], [2] and [6] for K a Dirichlet character.

Based on this thesis, various results that were proved only for prime moduli using the results of [22] should be easy to extend to squarefree moduli. Examples of such results can be found in [11] and [1].

1.1. Outline

In Section 2.6 we will state the main results of this thesis, which is that Fourier coefficients of modular forms or Eisenstein series do not correlate with some special functions defined on $\mathbb{Z}/q\mathbb{Z}$ for q squarefree. Furthermore, we present a similar result for sums over primes. For this, we will first give all definitions necessary and then state the precise results.

In Section 3 we will use the amplification method to reduce the main result to an estimate of amplified second moments. We follow closely [22], and embed the holomorphic form f in the space of forms of level qN. The amplification method itself is a well known tool and was well used before, e.g., by H. Iwaniec, V.A. Bykovsky, V. Blomer, G. Harcos and others (see [13], [6], [5], [2] and [3]). The amplifier used in [22] which we will adopt, goes back to Venkatesh.

In Section 4 and 5 we estimate the amplified second moments. The general strategy is based on [22]. However, especially the estimate of the number of correlation matrices (Section 5.7) is different from the method used in [22], as the original method does not generalize well to the squarefree case. Since this section is also quite intricate, we present in Section 5.7.3 a simplified version, where we assume that the only correlation matrix is the identity matrix, a case which is also common in applications.

In Section 6 we consider sums over primes to squarefree moduli, which is a generalisation of [23]. As the proofs of the results in this section are based on previous results in this thesis and otherwise closely follow the proofs in [23] with only minor adaptions, we are quite brief in this section, but give detailed references.

Finally, in Section 7, we present as an application a proof of (1.2) mentioned in the introduction.

1.2. Acknowledgements

I thank my advisor Emmanuel Kowalski for supporting me throughout my doctorate in many ways: by suggesting me interesting problems, by answering my questions, by giving advice on how to approach problems. I also thank professor Étienne Fouvry for examining my thesis.

I would also like to thank my fellow doctoral students for interesting mathematical discussions.

1.3. Notation

We write $e(z) = e^{2\pi iz}$ for any $z \in \mathbb{C}$. We denote the greatest common divisors of two integers a and b by (a, b). Furthermore we write

$$(a, b^\infty) = \max_{n\in\mathbb{N}} (a, b^n).$$

Concerning modular arithmetic, for $a \in \mathbb{Z}$ and $n \geq 1$ with $(a, n) = 1$, we write $\overline{a}$ for the inverse of a modulo n. The modulus n is always clear in context. On the other hand, for $a \mid b$, we write $\frac{b}{a}$ for the ordinary division in $\mathbb{Z}$. For example, if

$$b \equiv an \mod n^2$$

we know that the integer b is divisible by n and hence we can rewrite this congruence as

$$\frac{b}{n} \equiv a \mod n.$$

The notation $n \sim N$ means that $n \in \mathbb{Z}$ satisfies $N < n \leq 2N$.

2. Statement of Main Results

2.1. Preliminary definitions

We define a ***cusp form*** $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ as in [22]: By saying that f is a cusp form we will mean that f is either

(i) a non-zero holomorphic cusp form of some even weight $k \geq 2$ and some level $N \geq 1$ or

(ii) a non-zero Maass cusp form of weight 0, level N and Laplace eigenvalue written $\frac{1}{4} + t_f^2$,

where we assume in both cases that f has trivial Nebentypus. Furthermore, by saying that a cusp form f of level N is a Hecke eigenform we will mean that f is an eigenfunction of the Hecke operators T_n with $(n, N) = 1$.

Let now f be a cusp form. We denote by $\rho_f(n)$ the (normalized) Fourier coefficients of f. The Fourier expansion at ∞ reads then

$$f(z) = \sum_{n\geq 1} \rho_f(n) n^{\frac{k-1}{2}} e(nz)$$

if f is holomorphic of weight k and

$$f(z) = \sum_{n\neq 0} \rho_f(n) \left|n\right|^{-\frac{1}{2}} W_{it_f}\big(4\pi \left|n\right| y\big) e(nx)$$

if f is a Maass form with Laplace eigenvalue $\frac{1}{4} + t_f^2$ where

$$W_{it}(y) = \frac{e^{-\frac{y}{2}}}{\Gamma(it + \frac{1}{2})} \int_0^\infty e^{-x} x^{it-\frac{1}{2}} \Big(1 + \frac{x}{y}\Big)^{it-\frac{1}{2}} dx$$

is a Whittaker function (see Equation (3.8) in [22]).

Definition 2.1.1. Lef f be a cusp form. We say that the sequence $(\varrho_f(n))_{n\geq 1}$ does ***not correlate*** with another bounded (or essentially bounded) sequence $(K(n))_{n\in\mathbb{N}}$ if

$$\sum_{n\leq x} \varrho_f(n) K(n) \ll_A x (\log x)^{-A}$$

for all $A \geq 1$. Otherwise, we say that $(\varrho_f(n))_{n\geq 1}$ ***correlates*** with $(K(n))_{n\in\mathbb{N}}$.

In practice it is often useful to work with smoothed sums instead of sharp ones. Apart from the fact that it is often easier to work with smoothed sums, the bounds one can obtain for the smoothed sums are often better than the bounds for the sharp sums.

Definition 2.1.2. Let q be a squarefree integer, $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ an arbitrary function, extended to all of $\mathbb{Z}$ by periodicity, $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ a cusp form and V a smooth compactly supported function on $[0, +\infty[\longrightarrow \mathbb{R}$. Then we write

$$\mathcal{S}(f, K; q) = \mathcal{S}_V(f, K; q) = \sum_{n\geq 1} \varrho_f(n) K(n) V(n/q).$$

Proposition 2.1.3 (Trivial bound for $\mathcal{S}_V(f,K;q)$)**.** *Let* q*,* K*,* f *and* V *be as in Definition 2.1.2. We have the bound*

$$\mathcal{S}_V(f,K;q) \ll_{f,V} q \max_{1\le n\le q} |K(n)|.$$

Proof. By Rankin-Selberg theory,

$$\sum_{n\le x} |\rho_f(n)|^2 = c_f x + O\big(x^{\frac{3}{5}}\big) \tag{2.1}$$

for some $c_f > 0$. Since V has compact support, there exists a constant $c_1 \in \mathbb{N}$ such that $V(x) = 0$ for all $x \ge c_1$. Hence $V\big(\frac{n}{q}\big) = 0$ for all $n \ge qc_1$. Therefore

$$\begin{aligned}\mathcal{S}_V(f,K;q) &= \sum_{n\ge1} \rho_f(n)K(n)V\Big(\frac{n}{q}\Big) = \sum_{n=1}^{c_1q} \rho_f(n)K(n)V\Big(\frac{n}{q}\Big)\\ &\le \left|\sum_{n=1}^{c_1q} \rho_f(n)K(n)V\Big(\frac{n}{q}\Big)\right|\end{aligned}$$

which is by Cauchy's inequality

$$\begin{aligned}&\le \left(\sum_{n=1}^{c_1q} \left|\rho_f(n)V\Big(\frac{n}{q}\Big)\right|^2 \sum_{n=1}^{c_1q} |K(n)|^2\right)^{\frac{1}{2}}\\ &\ll_V \left(\sum_{n=1}^{c_1q} |\rho_f(n)|^2 \sum_{n=1}^{c_1q} |K(n)|^2\right)^{\frac{1}{2}}\end{aligned}$$

and hence by (2.1) this is

$$\ll_{f,V} \left(q\sum_{n=1}^{c_1q} |K(n)|^2\right)^{\frac{1}{2}}$$

and by using the periodicity of K, we can further simplify this to

$$\begin{aligned}&\ll_{f,V} \left(q\sum_{n=1}^{q} |K(n)|^2\right)^{\frac{1}{2}} \le \left(q^2 \max_{1\le n\le q} |K(n)|^2\right)^{\frac{1}{2}}\\ &\le q \max_{1\le n\le q} |K(n)|.\end{aligned}$$

□

In this thesis, we will give in some cases a better bound of the form

$$\mathcal{S}_V(f,K;q) \ll q^{1-\delta}$$

for some $0 < \delta < \frac{1}{8}$, where the implied constant only depends on δ, f, V and some invariants of K. Clearly, to prove such a bound on $\mathcal{S}_V(f,K;q)$ one has to make some assumptions about f, K and V. We will now state the precise assumptions we need to make, so that we can state our main result (Theorem 2.6.1).

2.2. Assumptions on the function K

For the correlation sum to be small, it is natural to assume that the function K should be of "low complexity". The heuristic idea behind this is, that if K is a "simple function" (as opposite to "complex"), the function K is not able to correlate with the Fourier coefficients ρ_f well enough. We will see later that a class of such functions are trace functions with small/bounded conductor, where the conductor is the quantity which measures the complexity of the trace function. Below, we will give the technical definitions necessary to exactly specify what we mean by a "simple function" K – we will call such functions *good* (see Definition 2.2.7 below).

Definition 2.2.1. Let q be a squarefree integer. For any function $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ we define its ***Fourier transform*** by

$$\hat{K}(x) = \frac{1}{\sqrt{q}} \sum_{z \in \mathbb{Z}/q\mathbb{Z}} K(z) e\Big(\frac{zx}{q}\Big).$$

Definition 2.2.2. Let q be a squarefree number. We call a function $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ ***q-primeperiodic*** if for every $p \mid q$ there exists a function $K_p\colon \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{C}$ such that

$$K(x) = \prod_{p \mid q} K_p(x).$$

We extend the function to all of $\mathbb{Z}$ by periodicity.

Proposition 2.2.3. *Let q be a squarefree integer and let $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ be a q-primeperiodic function, i.e.,*

$$K(x) = \prod_{p \mid q} K_p(x).$$

Then

$$\hat{K}(x) = \prod_{p \mid q} \hat{K}_p(s_p x)$$

where

$$s_p \equiv \prod_{\substack{p' \mid q \\ p' \neq p}} \overline{p'} \in (\mathbb{Z}/p\mathbb{Z})^\times.$$

Proof. We compute

$$\begin{aligned}\hat{K}(x) &= \frac{1}{\sqrt{q}} \sum_{z \in \mathbb{Z}/q\mathbb{Z}} K(z) e\Big(\frac{zx}{q}\Big) \\ &= \frac{1}{\sqrt{q}} \sum_{z \in \mathbb{Z}/q\mathbb{Z}} e\Big(\frac{zx}{q}\Big) \prod_{p \mid q} K_p(z)\end{aligned}$$

Now, for all $p|q$, let $z_p \in \mathbb{Z}$ be such that $z_p \equiv z \in \mathbb{Z}/p\mathbb{Z}$. Then z can be written as

$$z = \sum_{p \mid q} z_p e_p \in \mathbb{Z}/q\mathbb{Z}$$

where $e_p = s_p \prod_{\substack{p' \mid q \\ p' \neq p}} p' \in \mathbb{Z}$ so that $e_p \equiv 1 \mod p$. Hence

$$\hat{K}(x) = \prod_{p \mid q} \frac{1}{\sqrt{p}} \sum_{z_p \in \mathbb{Z}/p\mathbb{Z}} e\Big(\frac{z_p e_p x}{q}\Big) K_p(z_p)$$

$$= \prod_{p|q} \frac{1}{\sqrt{p}} \sum_{z_p \in \mathbb{Z}/p\mathbb{Z}} e\Big(\frac{z_p s_p x}{p}\Big) K_p(z_p)$$
$$= \prod_{p|q} \hat{K}_p(s_p x).$$

□

Definition 2.2.4. Let q be a squarefree integer and

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/q\mathbb{Z}).$$

For any $x \in \mathbb{Z}/q\mathbb{Z}$ such that $cx + d$ is invertible in $\mathbb{Z}/q\mathbb{Z}$, we define the action

$$\gamma \cdot x = \frac{ax + b}{cx + d} \in \mathbb{Z}/q\mathbb{Z}.$$

We then define for a function $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ and a matrix $\gamma \in M_2(\mathbb{Z}/q\mathbb{Z})$ the ***correlation sum***

$$\mathcal{C}(K;\gamma) = \sum_{\substack{x \in \mathbb{Z}/q\mathbb{Z} \\ cx+d \in (\mathbb{Z}/q\mathbb{Z})^\times}} \hat{K}(\gamma \cdot x)\overline{\hat{K}(x)}.$$

Proposition 2.2.5. *Let q be a squarefree integer and let $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ be a q-primeperiodic function. Then*

$$\mathcal{C}(K;\gamma) = \prod_{p|q} \mathcal{C}\big(K_p;\gamma_p\big)$$

where

$$\gamma_p = \begin{pmatrix} a & bs_p \\ c\overline{s_p} & d \end{pmatrix} \qquad\qquad s_p \equiv \prod_{\substack{p'|q \\ p' \neq p}} \overline{p'} \mod p.$$

Proof. We have

$$\mathcal{C}(K;\gamma) = \sum_{\substack{x \in \mathbb{Z}/q\mathbb{Z} \\ cx+d \in (\mathbb{Z}/q\mathbb{Z})^\times}} \hat{K}(\gamma \cdot x)\overline{\hat{K}(x)}$$

which is by Proposition 2.2.3 equal to

$$= \sum_{\substack{x \in \mathbb{Z}/q\mathbb{Z} \\ cx+d \in (\mathbb{Z}/q\mathbb{Z})^\times}} \prod_{p|q} \hat{K}_p(s_p\gamma \cdot x)\overline{\hat{K}_p(s_p x)}$$
$$= \sum_{\substack{x \in \mathbb{Z}/q\mathbb{Z} \\ cx+d \in (\mathbb{Z}/q\mathbb{Z})^\times}} \prod_{p|q} \hat{K}_p(s_p\gamma \cdot x_p)\overline{\hat{K}_p(s_p x_p)},$$

where we denote by x_p the reduction of x modulo p. Hence, by the Chinese remainder theorem,

$$\mathcal{C}(K;\gamma) = \prod_{p|q} \sum_{\substack{x_p \in \mathbb{F}_p \\ cx_p+d \in \mathbb{F}_p^\times}} \hat{K}_p(s_p\gamma \cdot x_p)\overline{\hat{K}_p(s_p x_p)}.$$

Since

$$s_p\gamma \cdot x_p = \frac{as_px_p + bs_p}{cx_p + d} = \frac{as_px_p + bs_p}{c\overline{s_p}s_px_p + d} = \gamma_p \cdot (s_px_p)$$

we get by putting $y_p = s_px_p$

$$\begin{aligned}\mathcal{C}(K;\gamma) &= \prod_{p|q} \sum_{\substack{y_p \in \mathbb{F}_p \\ c_py_p + d \in \mathbb{F}_p^\times}} \hat{K}_p(\gamma_p \cdot y_p)\overline{\hat{K}_p(y_p)} \\ &= \prod_{p|q} \mathcal{C}(K_p;\gamma_p),\end{aligned}$$

which completes the proof. □

Lemma 2.2.6 (Trivial bound for $\mathcal{C}(K;\gamma)$). *Let $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ with $\|K\|_\infty \leq M$ and let $\gamma \in \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$. We then have the bound*

$$|\mathcal{C}(K;\gamma)| \leq M^2 q.$$

Proof. By the Cauchy-Schwarz inequality, we can bound

$$\begin{aligned}|\mathcal{C}(K;\gamma)|^2 &= \Bigg| \sum_{\substack{z\in\mathbb{Z}/q\mathbb{Z} \\ (cz+d,q)=1}} \hat{K}(\gamma\cdot z)\overline{\hat{K}(z)}\Bigg|^2 \leq \sum_{\substack{z\in\mathbb{Z}/q\mathbb{Z} \\ (cz+d,q)=1}} \left|\hat{K}(\gamma\cdot z)\right|^2 \sum_{\substack{u\in\mathbb{Z}/q\mathbb{Z} \\ (cu+d,q)=1}} \left|\hat{K}(u)\right|^2 \\ &= \sum_{\substack{z\in\mathbb{Z}/q\mathbb{Z} \\ (cz-a,q)=1}} \left|\hat{K}(z)\right|^2 \sum_{\substack{u\in\mathbb{Z}/q\mathbb{Z} \\ (cu+d,q)=1}} \left|\hat{K}(z)\right|^2 \leq \sum_{z\in\mathbb{Z}/q\mathbb{Z}} \left|\hat{K}(z)\right|^2 \sum_{u\in\mathbb{Z}/q\mathbb{Z}} \left|\hat{K}(u)\right|^2 \\ &= \Bigg(\sum_{z\in\mathbb{Z}/q\mathbb{Z}} \left|\hat{K}(z)\right|^2\Bigg)^2.\end{aligned}$$

Recall Parseval's formula

$$\begin{aligned}\sum_{z\in\mathbb{Z}/q\mathbb{Z}} \left|\hat{K}(z)\right|^2 &= \sum_{z\in\mathbb{Z}/q\mathbb{Z}} \left|\frac{1}{\sqrt{q}} \sum_{x\in\mathbb{Z}/q\mathbb{Z}} K(x)e\Big(\frac{zx}{q}\Big)\right|^2 = \frac{1}{q} \sum_{z\in\mathbb{Z}/q\mathbb{Z}} \sum_{x,y\in\mathbb{Z}/q\mathbb{Z}} K(x)\overline{K(y)}e\Big(\frac{z(x-y)}{q}\Big) \\ &= \frac{1}{q} \sum_{x,y\in\mathbb{Z}/q\mathbb{Z}} K(x)\overline{K(y)} \sum_{z\in\mathbb{Z}/q\mathbb{Z}} e\Big(\frac{z(x-y)}{q}\Big) = \sum_{x\in\mathbb{Z}/q\mathbb{Z}} K(x)\overline{K(x)} \\ &= \sum_{x\in\mathbb{Z}/q\mathbb{Z}} |K(x)|^2.\end{aligned}$$

Hence

$$|\mathcal{C}(K;\gamma)| \leq \sum_{z\in\mathbb{Z}/q\mathbb{Z}} |K(z)|^2 = \sum_{z\in\mathbb{Z}/q\mathbb{Z}} \left|\hat{K}(z)\right|^2 \leq M^2 q.$$

□

This bound is not sufficient to prove our main result. The idea is, that in most cases $\mathcal{C}(K;\gamma)$ should be much smaller according to the square-root cancellation philosophy. Unfortunately, this is not always the case. Fortunately, for the K's which we will consider[1] we have detailed

[1] Namely the good K's as defined in Definition 2.2.7.

knowledge about the set of γ's for which $\mathcal{C}(K;\gamma)$ fails to be small, in particular this set turns out to be small.

Note also the special case of $\hat{K}$ being constant and hence $K(n)$ being proportional to $e\big(\frac{an}{q}\big)$ for some $a \in \mathbb{Z}$. In this case $\mathcal{C}(K;\gamma)$ is never small and hence such a K will obviously not satisfy the assumptions of our main theorem. However, this case can be treated directly by different methods, see (1.3) in [22].

Notation. Given $x \neq y$ in $\mathbb{P}^1(\mathbb{F}_p)$, the pointwise stabilizer of x and y is denoted by $T^{x,y}(\mathbb{F}_p)$ (this is a maximal torus), and its normalizer in $\mathrm{PGL}_2(\mathbb{F}_p)$ (i.e. the stabilizer of the set $\{x,y\}$) is denoted by $N^{x,y}(\mathbb{F}_p)$.

Definition 2.2.7 (Correlation matrices and good weights)**.** Let $M \geq 1$ and let q be a squarefree number. For every $p \mid q$ let $K_p\colon \mathbb{F}_p \longrightarrow \mathbb{C}$ be an arbitrary functions with $\|K_p\|_2 \leq M$. Define $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ by $K = \prod_{p\mid q} K_p$. Furthermore, for $\gamma \in M_2(\mathbb{Z})$, we denote by γ_p its image in $\mathrm{PGL}_2(\mathbb{F}_p)$.

(i) We let

$$\mathbf{G}_{K_p,M} = \Big\{\gamma \in \mathrm{PGL}_2(\mathbb{F}_p) \;\Big|\; |\mathcal{C}(K_p;\gamma_p)| > Mp^{\frac{1}{2}}\Big\},$$

the set of M***-correlation matrices***.

(ii) We say that K_p is (p,M)***-good*** if there exists some set $\mathcal{D}_p$ of at most M pairs (x,y) of distinct elements in $\mathbb{P}^1(\mathbb{F}_p)$ such that

$$\mathbf{G}_{K,M} \subset \mathcal{A}_p = \bigcup_{i \in \mathcal{I}_p} \mathcal{A}_p^i$$

where

$$\mathcal{I}_p = \{1,2,3,4\} \cup \{(5,x,y) \mid (x,y) \in \mathcal{D}_p\} \cup \{(6,x,y) \mid (x,y) \in \mathcal{D}_p\}$$

and

(i) $\mathcal{A}_p^1 = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}$,

(ii) $\mathcal{A}_p^2 = \left\{\begin{pmatrix} 0 & * \\ * & * \end{pmatrix}\right\}$,

(iii) $\mathcal{A}_p^3 = \left\{\begin{pmatrix} * & * \\ * & 0 \end{pmatrix}\right\}$,

(iv) $\mathcal{A}_p^4 = \big\{A \in M_2(\mathbb{F}_p) \;\big|\; A \text{ is parabolic, i.e., has a single fixed point in } \mathbb{P}^1(\mathbb{F}_p)\big\}$,

(v) $\mathcal{A}_p^{(5,x,y)} = T^{x,y}(\mathbb{F}_p)$, and

(vi) $\mathcal{A}_p^{(6,x,y)} = N^{x,y}(\mathbb{F}_p) \setminus T^{x,y}(\mathbb{F}_p)$.

We call such a set $\mathcal{A}_p$ a set of ***admissible correlation matrices modulo*** p.

(vii) We say that K is (q,M)***-good***, if K_p is (p,M)-good for every $p \mid q$.

The conditions stated so far are enough to state the main Theorems 2.6.1 and 2.6.2. However, to successfully apply these main theorems to sums over primes to squarefree moduli, we need some more assumptions on K, as stated below.

Definition 2.2.8. For a function $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ and $(m,h) \in (\mathbb{Z}/q\mathbb{Z})^\times \times \mathbb{Z}/q\mathbb{Z}$, we define the ***correlation sum***

$$\mathcal{C}'\big(K;(m,h)\big) = \sum_{z \in \mathbb{Z}/q\mathbb{Z}} \overline{K(mz)}K(z)e\Big(\frac{hz}{q}\Big).$$

Proposition 2.2.9. *Let q be a squarefree integer and $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ a q-primeperiodic function given by*

$$K(z) = \prod_{p\mid q} K_p(z).$$

Then

$$\mathcal{C}'\big(K;(m,h)\big) = \prod_{p\mid q} \mathcal{C}'\big(K_p;(m,s_p h)\big)$$

where

$$s_p \equiv \prod_{\substack{p'\mid q\\ p'\neq p}} \overline{p'} \mod p.$$

Proof. We compute

$$\begin{aligned}
\mathcal{C}'\big(K;(m,h)\big) &= \sum_{z\in\mathbb{Z}/q\mathbb{Z}} \overline{K(mz)}K(z)e\Big(\frac{hz}{q}\Big)\\
&= \sum_{z\in\mathbb{Z}/q\mathbb{Z}} e\Big(\frac{hz}{q}\Big)\prod_{p\mid q}\overline{K_p(mz)}K_p(z)\\
&= \prod_{p\mid q}\sum_{z_p\in\mathbb{Z}/p\mathbb{Z}} e\Big(\frac{z_p e_p h}{q}\Big)\overline{K_p(mz_p)}K_p(z_p)\\
&= \prod_{p\mid q}\sum_{z_p\in\mathbb{Z}/p\mathbb{Z}} e\Big(\frac{z_p s_p h}{p}\Big)\overline{K_p(mz_p)}K_p(z_p)\\
&= \prod_{p\mid q}\mathcal{C}'\big(K_p;(m,s_p h)\big),
\end{aligned}$$

where we defined $e_p = s_p\prod_{p'\neq p} p' \in \mathbb{Z}$. □

Lemma 2.2.10 (Trivial bound for $\mathcal{C}'\big(K_p;(m,h)\big)$)**.** *We have for $K_p\colon \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{C}$ with $\|K\|_\infty \leq M$ the bound*

$$\big|\mathcal{C}'\big(K_p;(m,h)\big)\big| \leq M^2 p.$$

Proof. This can be seen by

$$\big|\mathcal{C}'\big(K_p;(m,h)\big)\big| \leq \sum_{z\in\mathbb{Z}/p\mathbb{Z}} \Big|\overline{K(mz)}\Big|\,|K(z)|\,\Big|e\Big(\frac{hz}{p}\Big)\Big| \leq \sum_{z\in\mathbb{Z}/p\mathbb{Z}} M^2 \leq M^2 p.$$

□

Definition 2.2.11. Let q be a squarefree number and $K_p\colon \mathbb{F}_p \longrightarrow \mathbb{C}$ be arbitrary functions for all $p \mid q$. Let $M \geq 1$ be such that $\|K_p\|_2 \leq M$. Define $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ by $K = \prod_{p\mid q} K_p$.

(i) We let

$$\mathbf{H}_{K_p,M} = \Big\{(m,h) \in \mathbb{F}_p^\times \times \mathbb{F}_p \;\Big|\; \big|\mathcal{C}'\big(K_p;(m,h)\big)\big| > Mp^{\frac{1}{2}}\Big\}$$

be the set of (p,M)-exceptional vectors.

(ii) We say that K_p is (p,M)-non-exceptional if

$$\big|\mathbf{H}_{K_p,M}\big| \leq M.$$

(iii) We say that K is (q,M)-non-exceptional if K_p is (p,M)-non-exceptional for every $p \mid q$.

2.3. Trace functions on ℓ-adic sheaves

For Theorem 2.6.1 to be useful, we need to check that it actually applies to functions

$$K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$$

which appear in practice. As shown in [22], trace functions as defined below turn out to be (p, M)-good functions. The exact definition of trace functions is given in [22, Section 1.3] and we will repeat it here for completeness only. Since we will not need to work with the definition of a trace function in this thesis, we will be relatively brief in what follows, but provide references where more details can be found. If one is only interest in applying the results of this thesis to concrete problems, it is often enough to know that certain special functions of interest are trace functions (with some small conductor). We will give some examples of such functions below.

We make the following definitions (compare Definition 1.11 in [22]):

(i) A constructible $\bar{\mathbb{Q}}_\ell$-sheaf $\mathcal{F}$ on $\mathbb{A}^1_{\mathbb{F}_p}$ is a trace sheaf if it is a middle-extension sheaf whose restriction to any non-empty open subset $U \subset \mathbb{A}^1_{\mathbb{F}_p}$ where $\mathcal{F}$ is lisse and pointwise ι-pure of weight 0.

(ii) A trace sheaf $\mathcal{F}$ which is also a Fourier sheaf in the sense of Katz [18, Definition 8.2.2] is called a Fourier trace sheaf.

(iii) A trace sheaf is an isotypic trace sheaf if it is a Fourier sheaf and if, for any open set U as in (i), the restriction of $\mathcal{F}$ to U is geometrically isotypic when seen as a representation of the geometric fundamental group of U: it is the direct sum of several copies of some (necessarily non-trivial) irreducible representation of the geometric fundamental group of U [18, Section 8.4].

Let p be a prime number and $\ell \neq p$ be an auxiliary prime. Consider an ℓ-adic constructible sheaf $\mathcal{F}$ on $\mathbb{A}^1_{\mathbb{F}_p}$ and fix an isomorphism $\iota\colon \bar{\mathbb{Q}}_\ell \longrightarrow \mathbb{C}$. For $x \in \mathbb{F}_p$, we define as in [19, 7.3.7]

$$K(x) = \iota\big((\mathrm{tr}\mathcal{F})(\mathbb{F}_p, x)\big). \tag{2.2}$$

A function $K\colon F_p \longrightarrow \mathbb{C}$ is a trace function (resp. Fourier trace function, isotypic trace function) if there is some trace sheaf (resp. Fourier trace sheaf, resp. isotypic trace sheaf) $\mathcal{F}$ on $\mathbb{A}^1_{F_p}$ such that K is given by (2.2).

As already mentioned in the introduction, we want a measure for the complexity of a trace function. It turns out, that the conductor as defined below is the right notion.

Definition 2.3.1. Let $\mathcal{F}$ be an ℓ-adic constructible sheaf $\mathcal{F}$ on $\mathbb{A}^1_{\mathbb{F}_p}$. We denote the rank of $\mathcal{F}$ by $\mathrm{rank}(\mathcal{F})$ and the (finite) number of singularities in $\mathbb{P}^1$ of $\mathcal{F}$ by $n(\mathcal{F})$. We define

$$\mathrm{Swan}(\mathcal{F}) = \sum_x \mathrm{Swan}_x(\mathcal{F}),$$

the (finite) sum being over all singularities of $\mathcal{F}$. The (analytic) conductor of $\mathcal{F}$ is then defined by

$$\mathrm{cond}(\mathcal{F}) = \mathrm{rank}(\mathcal{F}) + n(\mathcal{F}) + \mathrm{Swan}(\mathcal{F}).$$

The conductor of a trace function $K\colon \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{C}$ is defined as the smallest conductor of a trace sheaf $\mathcal{F}$ with trace function K.

A nice introduction to trace functions is [20]. We refer to the books of Katz, namely [18] and [19], for readers interested in full details.

In addition to the definitions above, which correspond to the definitions made in [22], we would like to extend the notion of trace functions to squarefree integers q. Hence, we will call a q-primeperiodic function $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ a trace function (resp. Fourier trace function, resp. isotypic trace function) if

$$K(x) = \prod_{p|q} K_p(x)$$

and for every $p|q$, K_p is a trace function (resp. Fourier trace function, resp. isotypic trace function) as defined above. By extending the definition of a trace function in this way to squarefree integers q, Theorem 1.14 in [22] becomes:

Theorem 2.3.2 (Trace functions are good)**.** *Let q be a squarefree number, $N \geq 1$ and $\mathcal{F} = (\mathcal{F}_p)_{p|q}$ be a family of isotypic trace sheaves $\mathcal{F}_p$ on $\mathbf{A}^1_{\mathbb{F}_p}$, with $\operatorname{cond}(\mathcal{F}_p) \leq N$ for all $p \mid q$. Let K be the corresponding isotypic trace function. Then K is (q, aN^s)-good for some absolute constants $a \geq 1$ and $s \geq 1$.*

Proof. Note that

$$K = \prod_{p|q} K_p$$

where K_p is the trace function of $\mathcal{F}_p$, $p|q$. By Theorem 1.14 in [22] we get that for every $p|q$, K_p is (p, aN^s)-good for some absolute constants $a \geq 1$ and $s \geq 1$. Hence K is (q, aN^s)-good. $\square$

Hence Theorem 2.6.1 applies to isotypic trace functions. We list now some examples of trace functions, taken from [22, Section 10].

Example 2.3.3. For q squarefree, $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ and $m \geq 2$, (normalized) hyper-Kloosterman sums in $m-1$ variables defined by

$$\operatorname{Kl}_m(a;q) = q^{-\frac{m-1}{2}} \sum_{\substack{x_1,\ldots,x_m \in (\mathbb{Z}/q\mathbb{Z})^\times \\ x_1\cdots x_m \equiv a \mod q}} e\Big(\frac{x_1 + \cdots + x_m}{q}\Big)$$

are irreducible trace functions with conductor $\leq 2m+1$.

We first have to check that $\operatorname{Kl}_m(a;q)$ is a q-primeperiodic functions. For every $p|q$ and every $i \in \{1, \ldots, m\}$, let $x_{i,p} \in \mathbb{Z}$ be such that $x_{i,p} \equiv x_i \mod p$. Then x_i can be written as

$$x_i = \sum_{p|q} x_{i,p} e_p \in \mathbb{Z}/q\mathbb{Z}$$

where $e_p = s_p \prod_{\substack{p'|q \\ p' \neq p}} p' \in \mathbb{Z}$ so that $e_p \equiv 1 \mod p$. Hence

$$\begin{aligned}
\operatorname{Kl}_m(a;q) &= \prod_{p|q} p^{-\frac{m-1}{2}} \sum_{\substack{x_{1,p},\ldots,x_{m,p} \in \mathbb{F}_p^\times \\ x_{1,p}\cdots x_{m,p} \equiv a \mod p}} e\Big(\frac{x_{1,p}e_p + \cdots + x_{m,p}e_p}{q}\Big) \\
&= \prod_{p|q} p^{-\frac{m-1}{2}} \sum_{\substack{x_{1,p},\ldots,x_{m,p} \in \mathbb{F}_p^\times \\ x_{1,p}\cdots x_{m,p} \equiv a \mod p}} e\Big(\frac{x_{1,p}s_p + \cdots + x_{m,p}s_p}{p}\Big) \\
&= \prod_{p|q} p^{-\frac{m-1}{2}} \sum_{\substack{x_{1,p},\ldots,x_{m,p} \in \mathbb{F}_p^\times \\ x_{1,p}\cdots x_{m,p} \equiv a s_p^m \mod p}} e\Big(\frac{x_{1,p} + \cdots + x_{m,p}}{p}\Big)
\end{aligned}$$

$$= \prod_{p|q} \mathrm{Kl}_m(as_p^m; p).$$

Thus, $\mathrm{Kl}_m(a;q)$ is a q-primeperiodic and it remains to check that all the $\mathrm{Kl}_m(as_p^m;p)$'s are irreducible trace functions (with conductor $\leq 2m+1$). But this was already shown [22, Section 10.3].

Example 2.3.4. Let q be a squarefree number and χ a Dirichlet character modulo q. Define

$$K(n) = \chi(n).$$

By the Chinese remainder theorem, we have a ring isomorphism

$$\varphi\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \bigoplus_{p|q} \mathbb{Z}/p\mathbb{Z},\ n \longmapsto (n_p)_{p|q},$$

where n_p is the reduction of n modulo p. Denote now by $n'_p \in \bigoplus_{p|q} \mathbb{Z}/p\mathbb{Z}$ the element given by

$$n'_{p,p'} = \begin{cases} n_p & \text{if } p' = p, \\ 1 & \text{otherwise.} \end{cases}$$

for $p'|q$. Hence

$$\varphi(n) = \prod_{p|q} n'_p.$$

Hence

$$\chi(n) = \prod_{p|q} \chi\big((\varphi^{-1}(n'_p)\big) = \prod_{p|q} \chi_p(n_p)$$

where $\chi_p(n_p) = \chi\big((\varphi^{-1}(n'_p)\big)$. It is an easy exercise to check that χ_p is a Dirichlet character modulo p. If all χ_p are non-trivial, we have by Section 10.1 of [22] that $K(n) = \chi(n)$ is an irreducible trace function with conductor ≤ 3.

To deal with sums over primes, we need the following analogous result to Theorem 2.3.2.

Theorem 2.3.5. *Let q be a squarefree number, $N \geq 1$ and $\mathcal{F} = (\mathcal{F}_p)_{p|q}$ be a family of irreducible and non-p-exceptional trace sheaves $\mathcal{F}_p$ on $\mathbf{A}^1_{\mathbb{F}_p}$, with* $\mathrm{cond}(\mathcal{F}_p) \leq N$ *for all $p \mid q$. Let K be the corresponding isotypic trace function. Then K is (q, aN^s)-non-exceptional for some absolute constants $a \geq 1$ and $s \geq 1$.*

Proof. Note that

$$K = \prod_{p|q} K_p$$

where K_p is the trace function of $\mathcal{F}_p$, $p|q$. By Proposition 3.1 in [23] we get that for every $p|q$, K_p is (p, aN^s)-non-exceptional for some absolute constants $a \geq 1$ and $s \geq 1$. Hence K is (q, aN^s)-non-exceptional. □

2.4. Assumptions on f

We quickly review some standard definitions

Definition 2.4.1. Let Γ be a finite index subgroup of the modular group $\mathrm{SL}_2(\mathbb{Z})$. A ***modular form of weight*** k for the group Γ is a function $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ satisfying the following three conditions:

(i) f is holomorphic;

(ii) for all $z \in \mathbb{H}$ and every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, $f\left(\dfrac{az+b}{cz+d}\right) = (cz+d)^k f(z)$;

(iii) f is holomorphic at the cusps (of $\Gamma\backslash\mathbb{H}^*$).

Definition 2.4.2. Let Γ be a finite index subgroup of the modular group $\mathrm{SL}_2(\mathbb{Z})$. A ***holomorphic cusp form of weight*** k for the group Γ is a modular form of weight k for the group Γ which vanishes at all cusps.

We define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N \right\},$$

which is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Definition 2.4.3. A ***modular form of weight*** k ***and level*** D is a modular form of weight k for the group $\Gamma_0(D)$.

Definition 2.4.4. A ***holomorphic cusp form of weight*** k ***and level*** D is a holomorphic cusp form of weight k for the group $\Gamma_0(D)$.

Definition 2.4.5. A ***Maass form*** (or ***Maass waveform***) of weight k for the group Γ is a smooth function $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ satisfying the following conditions:

(i) for all $z \in \mathbb{H}$ and every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$;

(ii) f is an eigenvector of the Laplace-Beltrami operator $\Delta = -y^2\Big(\dfrac{\partial^2}{\partial x^2} + \dfrac{\partial^2}{\partial y^2}\Big)$, i.e., $\Delta f = \lambda f$ for some $\lambda \in \mathbb{C}$;

(iii) f grows at most polynomially at the cusps of Γ, i.e., if $\gamma \cdot \infty$ is a cusp of Γ, there exists $C > 0$ and $n \in \mathbb{N}$ such that $|f(\gamma \cdot z)| \le Cy^n$ for $y \to \infty$ uniformly in x, where $z = x + iy$.

Definition 2.4.6. Let Γ be a finite index subgroup of the modular group $\mathrm{SL}_2(\mathbb{Z})$. A ***Maass cusp form*** of weight k for the group Γ is a Maass form of weight k for the group Γ which vanishes at all cusps.

Definition 2.4.7. A ***Maass form of weight*** k ***and level*** D is a Maass form of weight k for the group $\Gamma_0(D)$.

Definition 2.4.8. A ***Maass cusp form of weight*** k ***and level*** D is a Maass cusp form of weight k for the group $\Gamma_0(D)$.

Definition 2.4.9. In this thesis, by a ***cusp form*** f we will mean either

(i) a non-zero holomorphic cusp form of some even weight $k \ge 2$ and some level $N \ge 1$; or

(ii) a non-zero Maass cusp form of weight 0, level N and Laplace eigenvalue written $\frac{1}{4} + t_f^2$.

In both cases, we assume f has trivial Nebentypus for simplicity.

Definition 2.4.10. Let $\mathbb{M}_k$ be the space of entire modular forms of weight k and $\mathbb{S}_k$ the space of cusp forms of weight k. The mapping $\langle \cdot, \cdot \rangle \colon \mathbb{M}_k \times \mathbb{S}_k \longrightarrow \mathbb{C}$, given by

$$\langle f, g \rangle = \int_F f(z)\overline{g(z)} y^k \frac{dxdy}{y^2}$$

is called ***Petersson inner product***, where $z = x + iy$ and

$$F = \left\{ z \in \mathbb{H} \,\middle|\, |\mathrm{Re}\, z| \leq \frac{1}{2}, |z| \geq 1 \right\}$$

is a fundamental region of the modular group Γ.

Definition 2.4.11. For a cusp form g of level D, we define the ***Petersson norm*** by

$$\|g\|_D^2 = \int_{\Gamma_0(D)\backslash\mathbb{H}} |g(z)|^2 \, y^{k_g} \frac{dxdy}{y^2}$$

where k_g is the weight for g holomorphic and $k_g = 0$ if g is a Maass form.

Definition 2.4.12. Let $q \geq 1$ be an integer and $k \geq 2$ an even integer. We make the following definitions:

(i) we denote by $\mathcal{S}_k(D)$ the Hilbert space (with respect to the Petersson inner product) of holomorphic cusp forms of weight k, level D and trivial Nebentypus;

(ii) we denote by $\mathcal{L}^2(D)$ the Hilbert space (with respect to the Petersson inner product) of Maass forms of weight 0, level D and trivial Nebentypus;

(iii) we denote by $\mathcal{L}_0^2(D) \subset \mathcal{L}^2(D)$ the Hilbert space (with respect to the Petersson inner product) of Maass cusp forms of weight 0, level D and trivial Nebentypus;

These spaces are endowed with the action of the commutative algebra $\mathbf{T}$ generated by the Hecke operators $\{T_n \mid n \geq 1\}$, where

$$T_n g(z) = \frac{1}{\sqrt{n}} \sum_{\substack{ad=n \\ (a,D)=1}} \left(\frac{a}{d}\right)^{\frac{k_g}{2}} \sum_{0 \leq b < d} g\left(\frac{az+b}{d}\right),$$

where $k_g = 0$ if $g \in \mathcal{L}^2(q)$ and $k_g = k$ if $g \in \mathcal{S}_k(D)$.

Definition 2.4.13. We say that a cusp form f is ***admissible***, if it satisfies the following properties:

(i) f is an eigenform of all Hecke operators T_n with $(n, qN) = 1$, where N denotes the level of f;

(ii) f is L^2-normalized with respect to the Petersson inner product.

Lemma 2.4.14. *The operators T_n with $(n, D) = 1$ are self-adjoint.*

Proof. We have to show that $\langle T_n g, h\rangle = \langle g, T_n h\rangle$ for all $g, h \in \mathcal{L}^2(D)$ or $\mathcal{S}_k(D)$. We compute for $g, h \in \mathcal{S}_k(D)$

$$\begin{aligned}
\langle T_n g, h\rangle &= \int_F T_n g(z)\overline{h(z)} y^k \frac{dxdy}{y^2} \\
&= \int_k \frac{1}{\sqrt{n}} \sum_{\substack{ad=n \\ (a,D)=1}} \left(\frac{a}{d}\right)^{\frac{k}{2}} \sum_{0 \leq b < d} g\left(\frac{az+b}{d}\right) \overline{h(z)} y^k \frac{dxdy}{y^2} \\
&= \int_k \frac{1}{\sqrt{n}} \sum_{\substack{ad=n \\ (a,D)=1}} \left(\frac{a}{d}\right)^{\frac{k}{2}} \sum_{0 \leq b < d} d^k g(z)\overline{h(z)} y^k \frac{dxdy}{y^2}
\end{aligned}$$

$$= \int_k g(z) \overline{\frac{1}{\sqrt{n}} \sum_{\substack{ad=n \\ (a,D)=1}} \left(\frac{a}{d}\right)^{\frac{k}{2}} \sum_{0\leq b<d} h\left(\frac{az+b}{d}\right)} y^k \frac{dxdy}{y^2}$$
$$= \langle g, T_n h\rangle.$$

□

Definition 2.4.15. The operators $\{T_n \mid (n,D)=1\}$ generate a subalgebra of $\mathbf{T}$, which we denote by $\mathbf{T}^{(D)}$. A ***(Hecke) eigenform*** of $\mathbf{T}^{(D)}$ is a modular form which is an eigenvector for all Hecke operators in $\mathbf{T}^{(D)}$.

Therefore, the spaces $\mathcal{S}_k(D)$ and $\mathcal{L}_0^2(D)$ have an orthonormal basis made of eigenforms of $\mathbf{T}^{(D)}$ which contain all L^2-normalized Hecke newforms. Such bases are denoted by $\mathcal{B}_k(D)$ and $\mathcal{B}(D)$, respectively.

Lemma 2.4.16. *For $\ell_1 \neq \ell_2$ prime numbers, we have that $T_{\ell_1}T_{\ell_2}f = T_{\ell_1\ell_2}f$ and hence $\lambda_f(\ell_1)\lambda_f(\ell_2) = \lambda_f(\ell_1\ell_2)$, where $f \in \mathcal{S}_k(D)$ or $f \in \mathcal{L}_0^2(D)$.*

Proof. We compute for $f \in \mathcal{S}_k(D)$

$$T_{\ell_1}T_{\ell_2}f(z) = \frac{1}{\sqrt{\ell_1}} \sum_{\substack{a_1d_1=\ell_1 \\ (a_1,D)=1}} \left(\frac{a_1}{d_1}\right)^{\frac{k_f}{2}} \sum_{0\leq b_1<d_1} \frac{1}{\sqrt{\ell_2}} \sum_{\substack{a_2d_2=\ell_1 \\ (a_2,D)=1}} \left(\frac{a_2}{d_2}\right)^{\frac{k_f}{2}} \sum_{0\leq b_2<d_2} d_1^k d_2^k f(z)$$
$$= \frac{1}{\sqrt{\ell_1\ell_2}} \sum_{\substack{a_1d_1=\ell_1 \\ (a_1,D)=1}} \sum_{\substack{a_2d_2=\ell_1 \\ (a_2,D)=1}} \left(\frac{a_1a_2}{d_1d_2}\right)^{\frac{k_f}{2}} \sum_{0\leq b_1<d_1} \sum_{0\leq b_2<d_2} (d_1d_2)^k f(z)$$

and by using that $(\ell_1,\ell_2)=1$, this is

$$= \frac{1}{\sqrt{\ell_1\ell_2}} \sum_{\substack{ad=\ell_1\ell_2 \\ (a,D)=1}} \left(\frac{a}{d}\right)^{\frac{k_f}{2}} \sum_{0\leq b<d} d^k f(z)$$
$$= T_{\ell_1\ell_2}f(z),$$

and analogous for $f \in \mathcal{L}_0^2(D)$. □

We denote by $\mathcal{E}(D)$ the ***Eisenstein spectrum***. The spectral expansion for $\psi \in \mathcal{E}(q)$ can be written

$$\psi(z) = \sum_{\chi} \sum_{g\in\mathcal{B}(\chi)} \int_{\mathbb{R}} \langle \psi, E_{\chi,g}(z,t)\rangle E_{\chi,g}(z,t) \frac{dt}{4\pi}.$$

This and the following proposition are explained in more detail in [22] in Section 3.1.1.

Proposition 2.4.17. *For $(n,q)=1$ and $T_n \in \mathbf{T}^{(q)}$, we have that the $E_{\chi,g}(t)$ are eigenvectors of T_n with eigenvalue*

$$\lambda_\chi(n,t) = \sum_{ab=n} \chi(a)\overline{\chi(b)} \left(\frac{a}{b}\right)^{it},$$

i.e.,

$$T_nE_{\chi,g}(t) = \lambda_\chi(n,t)E_{\chi,g}(t).$$

2.5. Assumptions on V

Definition 2.5.1. Let $P > 0$ and $Q \geq 1$ be real numbers and let $C = (C_\nu)_{\nu \geq 0}$ be a sequence of non-negative real numbers. A smooth compactly supported function V on $[0, +\infty[$ satisfies ***Condition*** $(V(P, Q, C))$ if

(i) The support of V is contained in the interval $[P, 2P]$;

(ii) For all $x > 0$ and all integers $\nu \geq 0$ we have the inequality $\left| x^\nu \dfrac{d^\nu}{dx^\nu} V(x) \right| \leq C_\nu Q^\nu$.

In the remainder of this thesis and we will often simply write $V(P, Q)$ instead of $V(P, Q, C)$ and not mention the dependence on C at all. Also note that later on, we will introduce another quantity denoted C, which should not be confused with the one used in the above definition. Following this convention makes the notation more consistent with the one in [22].

2.6. The main theorems

We will prove the following results, which are a generalisation of [22, Theorem 1.9] and [23, Theorem 1.15].

Theorem 2.6.1 (Bounds for good twists of cusp forms)**.** *Let $P > 0$, $Q \geq 1$ and $M \geq 1$ be real numbers. Let f be an admissible cusp form, $q \geq 1$ a squarefree number and V a function satisfying Condition $(V(P, Q, C))$. Let $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ be a (q, M)-good q-primeperiodic function. Then*

$$\mathcal{S}_V(f, K; q) \ll M^{\omega(q)} q^{1-\delta} (PQ)^{\frac{1}{2}} (P + 1)^{\frac{1}{2} + \frac{1}{8} - \delta} Q,$$

for any $\delta < \frac{1}{8}$, where the implied constant depends only on (f, δ, C).

Theorem 2.6.2 (Bounds for good twists of Eisenstein series)**.** *Let $P > 0$ and $Q \geq 1$ be real numbers and let V be a functions satisfying condition $(V(P, Q, C))$. Let q be a squarefree integer and let $K_p\colon \mathbb{F}_p \longrightarrow \mathbb{C}$ be a function for every $p \mid q$. Define $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ by*

$$K(z) = \prod_{p \mid q} K_p(z).$$

Assume that K is (q, M)-good. Then

$$\mathcal{S}_V(E_{\chi,f}(t), K; q) = \sum_{n \geq 1} d_{it}(n) K(n) V\Big(\frac{n}{q}\Big) \ll_{\eta, C, M} (1 + |t|)^A QP \Big(1 + \frac{1}{P}\Big)^{\frac{1}{2}} q^{1-\eta}$$

for any $\eta < \frac{1}{8}$ and for some $A \geq 1$ possibly depending on η.

In this thesis, we will focus on the proof of Theorem 2.6.1 and only sketch the proof of Theorem 2.6.2. Concerning applications, we are interested in sums over primes. By Theorem 2.3.5, the following theorem is a generalization of Theorem 1.5 in [23].

Theorem 2.6.3 (Trace weights vs. primes)**.** *Let $P > 0$ and $Q \geq 1$ be real numbers and let V be a functions satisfying condition $(V(P, Q, C))$. Let q be a squarefree integer and let $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ be a q-primeperiodic function. Assume that K is (q, M)-good and (q, M)-non-exceptional. Then*

$$\sum_n \Lambda(n) K(n) V\Big(\frac{n}{q}\Big) \ll_{\eta, M, C} QP \Big(1 + \frac{1}{P}\Big)^{\frac{1}{6}} q^{1-\eta}$$

for any $\eta < \frac{1}{24}$.

The proof of this theorem is carried out in Section 6. An application of this result is presented in Section 7.

3. Proof of Theorem 2.6.1

To give the proof of Theorem 2.6.1, we need some technical results presented in the next subsection. The actual proof is then carried out in Section 3.2.

3.1. Statement of the main technical results

By viewing f as being of level 2 or 3 if $N = 1$, we can assume that $N \geq 2$.

Lemma 3.1.1. *Let f be an admissible form. Then f is a cusp form with respect to the smaller congruence subgroup $\Gamma_0(qN)$ and the function*

$$\frac{f(z)}{[\Gamma_0(N) : \Gamma_0(qN)]^{\frac{1}{2}}} = \frac{f(z)}{(q+1)^{\frac{1}{2}}}$$

may therefore be embedded in a suitable orthonormal basis of modular cusp forms of level $D = qN$, which we denote either $\mathcal{B}(D)$ or $\mathcal{B}_{k_f}(D)$.

Definition 3.1.2. For coefficients $(b_\ell)_{L \leq \ell \leq 2L}$ and any modular form h, we define the ***amplifier*** $B(h)$ by

$$B_{(b_\ell)}(L; h) = \sum_{L \leq \ell \leq 2L} b_\ell \lambda_h(\ell).$$

We also use the notation $B_{(b_\ell),\chi}(L; g, t) = B_{(b_\ell)}(L; E_{g,\chi}(t))$, where χ is a Dirichlet character modulo N and $g \in \mathcal{B}(\chi)$.

Definition 3.1.3. We define for any even integer $k \geq 2$

$$M(L; k) = \frac{(k-2)!}{\pi(4\pi)^{k-1}} \sum_{g \in \mathcal{B}_k(D)} |B(L; g)|^2 \, |\mathcal{S}(g, K, q)|^2$$

and

$$M(L) = M^{\text{Hol}}(L) + M^{\text{Maa}}(L) + M^{\text{Eis}}(L)$$

where

$$M^{\text{Hol}}(L) = \sum_{\substack{k>0 \\ k \text{ even}}} \dot{\phi}_{a,b}(k)(k-1)M(L; k)$$

$$M^{\text{Maa}}(L) = \sum_{g \in \mathcal{B}(D)} \tilde{\phi}_{a,b}(t_g) \frac{4\pi}{\cosh(\pi t_g)} |B(L; g)|^2 \, |\mathcal{S}(g, K, q)|^2$$

$$M^{\text{Eis}}(L) = \sum_{\chi} \sum_{g \in \mathcal{B}(\chi)} \int_{-\infty}^{\infty} \tilde{\phi}_{a,b}(t) \frac{1}{\cosh(\pi t)} |B(L; g, t)|^2 \, |\mathcal{S}(E_{\chi,g}(t), K, q)|^2 \, dt$$

where $\phi_{a,b}$ is given by Definition A.0.8. $M^{\text{Hol}}(L)$, $M^{\text{Maa}}(L)$ and $M^{\text{Eis}}(L)$ are called the ***holomorphic, Maass*** and ***Eisenstein contributions of*** $M(L)$.

Proposition 3.1.4 (Bounds for the amplified moment)**.** *Let $P > 0$ and $Q \geq 1$ be real numbers, let $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ be an admissible cusp form and let $V\colon (0,\infty) \longrightarrow \mathbb{R}$ be a smooth compactly supported function satisfying Condition $(V(P,Q))$. Further, let $q \geq 1$ be a squarefree integer and let $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ be a (q,M)-good q-primeperiodic function. Then for any $\varepsilon > 0$ and any $L > 0$ with*

$$q^{\varepsilon} LQ < q^{\frac{1}{4}},$$

we have that for all sequences of complex numbers (b_ℓ) supported on primes ℓ with $L \leq \ell \leq 2L$ and such that $|b_\ell| \leq 2$ for all ℓ, the following holds: There exists $k(\varepsilon) \geq 2$, such that for all $k \geq k(\varepsilon)$ and all integers $a > b > 2$ satisfying

$$a - b \geq k(\varepsilon), \quad a \equiv b \equiv 1 \mod 2,$$

we have that

$$M(L), k^{-3}M(L;k) \ll_{\varepsilon,a,b,f} (q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}.$$

The implied constants depend on (ε, a, b, f), but they are independent of k. Note that $M(L)$ depends also on V, K, q and f.

3.2. Back to the proof of Theorem 2.6.1

We now give a proof of Theorem 2.6.1. So assume P, Q, f, q, V and K are given as in Theorem 2.6.1. Set

$$b_\ell = \begin{cases} \operatorname{sign}(\lambda_f(\ell)) & \text{if } \ell \nmid qN \text{ is a prime with } L \leq \ell \leq 2L \text{ and } \lambda_f(\ell) \neq 0, \\ 0 & \text{otherwise,} \end{cases} \tag{3.1}$$

where λ_f denotes the Hecke eigenvalues of f. Hence $b_\ell \in \{-1, 0, 1\}$ and we get for all ℓ the trivial bound $|b_\ell| \leq 1$. Fix $\varepsilon > 0$. Now, Proposition 3.1.4 gives us a $k(\varepsilon) \geq 2$.

Lemma 3.2.1. *For a cusp form f which is a Hecke eigenform, we have*

$$(q+1)^{-1} |B(f)|^2 |\mathcal{S}(f,K;q)|^2 \ll (q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}. \tag{3.2}$$

For a Eisenstein series $E_{\chi,h}$ which is a Hecke eigenform, we have

$$\int_{-\infty}^{\infty} \min\left(|t|^2, |t|^{-2-2b}\right) |B(h,t)|^2 |\mathcal{S}_V(E_{\chi,f}(t),K,q)|^2 \, dt$$
$$\ll q(q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}.$$

Proof. We will apply Proposition 3.1.4. Let $\varepsilon > 0$ and let

$$L = \frac{1}{2} q^{\frac{1}{4}-\varepsilon} Q^{-1}. \tag{3.3}$$

Then

$$q^{\varepsilon} LQ = \frac{1}{2} q^{\frac{1}{4}} < q^{\frac{1}{4}}.$$

Furthermore, let $k(\varepsilon)$ as in Proposition 3.1.4 and let $a > b \geq 2$ be odd integers, large enough (depending on ε), such that $a - b \geq k(\varepsilon)$. Hence the assumptions of Proposition 3.1.4 are satisfied and we get that

$$M(L), k^{-3}M(L;k) \ll_{\varepsilon,a,b,f} (q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}. \tag{3.4}$$

By Proposition A.0.9, we see that all summands of $M(L)$ are non-negative, except that for $a-b<k\leq a+b$, where some of the $\dot{\phi}(k)$ may be negative. By adding

$$2\sum_{\substack{a-b<k\leq a+b\\ \dot{\phi}(k)>0}}\left|\dot{\phi}(k)\right|(k-1)M(L;k)$$

to $M(L)$, we get a sum with only non-negative summands, i.e., we have

$$\begin{aligned}
M(L)+2&\sum_{\substack{a-b<k\leq a+b\\ \dot{\phi}(k)>0}}\left|\dot{\phi}(k)\right|(k-1)M(L;k)\\
&=\sum_{\substack{k>0\\ k\text{ even}}}\left|\dot{\phi}_{a,b}(k)\right|(k-1)M(L;k)+\sum_{g\in\mathcal{B}(D)}\tilde{\phi}_{a,b}(t_g)\frac{4\pi}{\cosh(\pi t_g)}\left|B(g)\right|^2\left|\mathcal{S}(g,K,q)\right|^2\\
&\quad+\sum_{\chi}\sum_{g\in\mathcal{B}(\chi)}\int_{-\infty}^{\infty}\tilde{\phi}_{a,b}(t)\frac{1}{\cosh(\pi t)}\left|B(g,t)\right|^2\left|\mathcal{S}(E_{\chi,g}(t),K,q)\right|^2dt
\end{aligned}$$

On the other hand, we have by Proposition A.0.9 that

$$\begin{aligned}
M(L)+2&\sum_{\substack{a-b<k\leq a+b\\ \dot{\phi}(k)>0}}\left|\dot{\phi}(k)\right|(k-1)M(L;k)\\
&\ll M(L)+2\sum_{\substack{a-b<k\leq a+b\\ \dot{\phi}(k)>0}}\frac{k-1}{k^{2b+2}}M(L;k)\\
&\ll M(L)+2\sum_{\substack{a-b<k\leq a+b\\ \dot{\phi}(k)>0}}k^{-3}M(L;k)
\end{aligned}$$

which, using Proposition 3.1.4, can be estimated as

$$\begin{aligned}
&\ll_{\varepsilon,a,b,f}\left(1+\sum_{a-b<k\leq a+b}1\right)(q^{1+\varepsilon}L^{1+\varepsilon}+q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}\\
&\ll_{\varepsilon,a,b,f}(q^{1+\varepsilon}L^{1+\varepsilon}+q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}.
\end{aligned}$$

Hence

$$\begin{aligned}
&\sum_{\substack{k>0\\ k\text{ even}}}\left|\dot{\phi}_{a,b}(k)\right|(k-1)M(L;k)+\sum_{g\in\mathcal{B}(D)}\tilde{\phi}_{a,b}(t_g)\frac{4\pi}{\cosh(\pi t_g)}\left|B(g)\right|^2\left|\mathcal{S}(g,K,q)\right|^2\\
&+\sum_{\chi}\sum_{g\in\mathcal{B}(\chi)}\int_{-\infty}^{\infty}\tilde{\phi}_{a,b}(t)\frac{1}{\cosh(\pi t)}\left|B(g,t)\right|^2\left|\mathcal{S}(E_{\chi,g}(t),K,q)\right|^2dt\\
&\quad\ll(q^{1+\varepsilon}L^{1+\varepsilon}+q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}
\end{aligned}\tag{3.5}$$

with all terms non-negative. In particular

$$\sum_{g\in\mathcal{B}(D)}\tilde{\phi}_{a,b}(t_g)\frac{4\pi}{\cosh(\pi t_g)}\left|B(g)\right|^2\left|\mathcal{S}(g,K,q)\right|^2\ll_{\varepsilon,a,b,f}(q^{1+\varepsilon}L^{1+\varepsilon}+q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)},$$

and if $\tilde{f} = \frac{f}{\sqrt{q+1}} \in \mathcal{B}(D)$,

$$\tilde{\phi}_{a,b}(t_{\tilde{f}}) \frac{4\pi}{\cosh(\pi t_{\tilde{f}})} \left|B(\tilde{f})\right|^2 \left|\mathcal{S}(\tilde{f}, K, q)\right|^2 \ll_{\varepsilon,a,b,f} (q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}.$$

Consequently, since $(q+1)^{-\frac{1}{2}}\mathcal{S}(f, K, q) = \mathcal{S}(\tilde{f}, K, q)$ and $B(f) = B(\tilde{f})$,

$$\tilde{\phi}_{a,b}(t_f) \frac{4\pi}{\cosh(\pi t_f)} (q+1)^{-1} \left|B(f)\right|^2 \left|\mathcal{S}(f, K, q)\right|^2 \\ \ll_{\varepsilon,a,b,f} (q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}.$$

Furthermore, because $t_f \in \mathbb{R} \cup (-i/4, i/4)$, we have that $\cosh(\pi t) \geq \frac{1}{2}$ and by Proposition A.0.9 that $\tilde{\phi}_{a,b}(t_f) \asymp (1+|t|)^{-2b-2}$. Thus

$$(q+1)^{-1} \left|B(f)\right|^2 \left|\mathcal{S}(f, K, q)\right|^2 \ll_{\varepsilon,a,b,f} (q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)},$$

which is equation (3.2) in the case where f is a Maass cusp form. If $\tilde{f} = \frac{f}{\sqrt{q+1}} \in \mathcal{B}_{k_f}(D)$, we analogously argue that

$$\sum_{\substack{k>0 \\ k \text{ even}}} \left|\dot{\phi}_{a,b}(k)\right| (k-1) \frac{(k-2)!}{\pi(4\pi)^{k-1}} \sum_{g \in \mathcal{B}_k(D)} \left|B(g)\right|^2 \left|\mathcal{S}(g, K, q)\right|^2 \\ \ll_{\varepsilon,a,b,f} (q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}$$

and a fortiori

$$\left|\dot{\phi}_{a,b}(k_f)\right| (k_f-1) \frac{(k_f-2)!}{\pi(4\pi)^{k_f-1}} \left|B(\tilde{f})\right|^2 \left|\mathcal{S}(\tilde{f}, K, q)\right|^2 \\ \ll_{\varepsilon,a,b,f} (q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}.$$

Again, this is

$$(q+1)^{-1} \left|B(f)\right|^2 \left|\mathcal{S}(f, K, p)\right|^2 \ll_{\varepsilon,a,b,f} (q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)},$$

which also gives us equation (3.2) in the case where f is a holomorphic cusp form.

It remains to check the case where $\tilde{h} = \frac{h}{\sqrt{q+1}}$ is in the Eisenstein spectrum $\mathcal{E}(q)$. Then there exists a characeter χ such that $h \in \mathcal{B}(\chi)$. By Proposition A.0.9, we get that

$$\begin{aligned} &\int_{-\infty}^{\infty} \min\left(|t|^2, |t|^{-2b-2}\right) \left|B(h,t)\right|^2 \left|\mathcal{S}(E_{\chi,h}(t), K, q)\right|^2 dt \\ &= (q+1) \int_{-\infty}^{\infty} \min\left(|t|^2, |t|^{-2b-2}\right) \left|B(\tilde{h},t)\right|^2 \left|\mathcal{S}(E_{\chi,\tilde{h}}(t), K, q)\right|^2 dt \\ &\ll q \int_{-\infty}^{\infty} (1+|t|)^{-2b-2} \left|B(\tilde{h},t)\right|^2 \left|\mathcal{S}(E_{\chi,\tilde{h}}(t), K, q)\right|^2 dt \\ &\ll q \int_{-\infty}^{\infty} \tilde{\phi}_{a,b}(t) \frac{1}{\cosh(\pi t)} \left|B(\tilde{h},t)\right|^2 \left|\mathcal{S}(E_{\chi,\tilde{h}}(t), K, q)\right|^2 dt \end{aligned}$$

which is by (3.5)

$$\ll q(q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}.$$

This completes the proof. □

Lemma 3.2.2. *For $L < q$ and (b_ℓ) given by* (3.1)*, we have for $B(f)$ as in Definition 3.1.2,*

$$B(f) \gg_f \frac{L}{(\log L)^4}$$

where the implied constant depends on f.

Proof. By the definition of $B(f)$, we have

$$B(f) = \sum_{\substack{L \le \ell \le 2L \\ \ell \nmid qN \\ \lambda_f(\ell) \neq 0}} \operatorname{sign}(\lambda_f(\ell))\lambda_f(\ell) = \sum_{\substack{L \le \ell \le 2L \\ \ell \nmid qN}} |\lambda_f(\ell)| \, .$$

If we let

$$\mathcal{L} = \left\{ \ell \sim L \;\middle|\; \ell \nmid qN, |\lambda_f(\ell)| > (\log L)^{-1} \right\},$$

then

$$\frac{L}{\log L} \ll \sum_{\substack{\ell \sim L \\ \ell \nmid qN}} |\lambda_f(\ell)|^2 \ll \frac{L}{(\log L)^3} + |\mathcal{L}|^{\frac{1}{2}} \left(\sum_{\ell \sim L} |\lambda_f(\ell)|^4 \right)^{\frac{1}{2}}$$

by the Prime Number Theorem for the Rankin-Selberg L-function $L(f \otimes f, s)$ (see e.g. [17, Theorem 5.44 and Theorem 5.13]) and the Cauchy-Schwarz inequality. By [21, (3.4)],

$$\sum_{\ell \sim L} |\lambda_f(\ell)|^4 \ll_f L \log L$$

and hence

$$\frac{L}{\log L} \ll_f \sqrt{|\mathcal{L}|}\sqrt{L \log L}.$$

Therefore

$$B(f) \geq \frac{|\mathcal{L}|}{\log L} \gg_f \frac{L}{(\log L)^4}.$$

□

We can now complete the proof of Theorem 2.6.1. By (3.2) we have that

$$|\mathcal{S}(f, K; q)|^2 \ll_{\varepsilon,a,b,f} (q+1)(q^{1+\varepsilon}L^{1+\varepsilon} + q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}\,|B(f)|^{-2}$$

which is by Lemma 3.2.2 and the definition of L

$$\ll_{\varepsilon,a,b,f} q^{\frac{7}{4}+\varepsilon}QP(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}(\log L)^8, \tag{3.6}$$

where we renamed ε.

Recall the definition of L by (3.3). We consider now the cases where $L \geq 1$ and $L < 1$ separately. First, if $L \geq 1$, we get by (3.6) that

$$\mathcal{S}(f, K; q) \ll_{\varepsilon,a,b,f} q^{\frac{7}{8}+\varepsilon}(PQ)^{\frac{1}{2}}(P+1)^{\frac{1}{2}+\frac{\varepsilon}{2}}QM^{\omega(q)}$$

since

$$\log(L) = \log\left(\frac{1}{2}q^{\frac{1}{4}-\varepsilon}Q^{-1}\right) = -\log(2) - \log(Q) + \left(\frac{1}{4} - \varepsilon\right)\log(q)$$

$$\leq \log(q) \ll_\varepsilon q^{\frac{\varepsilon}{2}}.$$

In the case $L < 1$, we have $Q > \frac{1}{2}q^{\frac{1}{4}-\varepsilon}$ and hence $q^{\frac{1}{8}-\frac{\varepsilon}{2}} \ll Q^{\frac{1}{2}}$. Consequently, by the trivial bound for $\mathcal{S}(f,K;q)$,

$$\mathcal{S}(f,K;q) \ll_{f,V} q \max_{1\leq n\leq q} |K(n)| \ll_{f,V} qM^{\omega(q)} \ll_{f,V} M^{\omega(q)} q^{\frac{7}{8}+\frac{\varepsilon}{2}} Q^{\frac{1}{2}}$$
$$\ll_{f,V} M^{\omega(q)} q^{\frac{7}{8}+\varepsilon}(PQ)^{\frac{1}{2}}(P+1)^{\frac{1}{2}+\frac{\varepsilon}{2}}Q.$$

This completes the proof of Theorem 2.6.1.

3.3. Sketch of the proof for Theorem 2.6.2

The proof of Theorem 2.6.2 is analogous to the proof of [23, Theorem 1.15]. In [23], the proofs of Theorem 1.15 and 1.16 are carried out simultaneously. Hence, we will now also state the generalized version of Theorem 1.16, which is actually the theorem which we will need later on, when we consider some applications.

Definition 3.3.1. We say that a test function V satisfies condition $V(Q)$ if it is compactly supported in $[\frac{1}{2}, 2]$ such that

$$x^j V^{(j)}(x) \ll Q^j$$

for some $Q \geq 1$ and for any integer $j \geq 0$, where the implicit constant depends on j.

Theorem 3.3.2. *Let q be a squarefree number and let $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ be a q-primeperiodic function. Assume that K is (q,M)-good. Let $P \geq 0$ be a parameter and define $X = Pq$. Let $M, N \geq 1$ be parameters with $\frac{X}{4} \leq MN \leq X$. Let U, V, W be smooth functions satisfying conditions $V(Q_U)$, $V(Q_V)$ and $V(Q_W)$ respectively, with $Q_U, Q_V, Q_W \geq 1$. Then, if q is big enough such that $q^{\frac{3}{4}} \leq X \leq q^{\frac{3}{2}}$, we have*

$$\sum_{m,n} K(mn)\Big(\frac{m}{n}\Big)^{it} U\Big(\frac{m}{M}\Big)V\Big(\frac{n}{N}\Big)W\Big(\frac{mn}{X}\Big) \ll \big(1+|t|\big)^A (Q_U+Q_V)^B Q_W X\Big(1+\frac{q}{X}\Big)^{\frac{1}{2}} q^{-\eta}$$

for $t \in \mathbb{R}$ and for any $\eta < \frac{1}{8}$ and for some constants A, $B \geq 1$ depending on η only. The implicit constant depends only on η, on the implicit constants in Definition 3.3.1, and polynomially on M.

We adapt the notation of [23] and define

$$\mathbf{P} = (U, V, W, M, N, X)$$

and

$$\mathcal{S}_{\mathbf{P}}(it, K) = \sum_{m,n} K(mn)\Big(\frac{m}{n}\Big)^{it} U\Big(\frac{m}{M}\Big)V\Big(\frac{n}{N}\Big)W\Big(\frac{mn}{X}\Big)$$

as well as

$$\mathcal{S}_{V,X}(it, K) = \sum_n K(n) d_{it}(n) V\Big(\frac{n}{X}\Big).$$

Furthermore, one should keep in mind that $X = Pq$. To prove Theorem 2.6.2 and Theorem 3.3.2 we follow the proof of Theorem 1.15 and 1.16 in [23] which is carried out there in section 2.

Lemma 2.1 of [23] holds without any modification for q squarefree instead of p prime as the proof is completely analytic. Furthermore, Lemma 2.2 is not needed in our case, as for q large enough compared to P, we have $q^{\frac{3}{4}} \leq X \leq q^{\frac{3}{2}}$, where $X = Pq$. Hence by assuming this, we can continue the proof following section 2.2 of [23]. Hence we define the amplifie

Definition 3.3.3. For $\tau \in \mathbb{R}$, $L \geq 1$ and $u \in \mathbb{C}$ we define the amplifier of length $2L$ adapted to the Eisenstein series $E(z, \frac{1}{2} + i\tau)$ by

$$B_{i\tau}(u) = \sum_{\substack{\ell \sim L \\ \ell \nmid qN \\ \ell \text{ prime}}} \operatorname{sign}\big(d_{i\tau}(\ell)\big) d_u(\ell).$$

Lemma 3.3.4. *For L large enough, we have*

$$B_{i\tau}(it) \gg \frac{L}{(\log L)^6},$$

uniformly for t and $\tau \in \mathbb{R}$ satisfying

$$|t - \tau| \ll \frac{1}{(\log L)^7} \qquad \textit{and} \qquad |\tau| \leq L^{\frac{1}{3}}.$$

For a proof, see [23, Lemma 2.4]. Since $B(h, t) = B_{i\tau}(it)$ for $h = E(z, \frac{1}{2} + it)$ and $f = (z, \frac{1}{2} + i\tau)$, Lemma 3.2.1 is a generalized version of Lemma 2.3 in [23]. We can then complete the proof of Theorem 2.6.2 completely analogous to the proof of [23, Theorem 1.15] as described on page 1706 – 1709 in [23].

4. Proof of Proposition 3.1.4

The aim of this section is to give a proof of Proposition 3.1.4. Recall that $M(L;k)$ and $M(L)$ are given by Definition 3.1.3. By defining

$$c_k = \frac{(k-2)!}{\pi(4\pi)^{k-1}}$$

we get that

$$M(L;k) = c_k \sum_{g\in\mathcal{B}_k(D)} \left|\sum_{\ell\sim L} b_\ell \lambda_g(\ell)\right|^2 \left|\sum_{n=1}^{\infty} \varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\right|^2,$$

where $D = qN$. Since $\lambda_g(\ell_1)$ and $\lambda_g(\ell_2)$ are real, we have

$$\begin{aligned} M(L;k) &= c_k \sum_{g\in\mathcal{B}_k(D)} \left|\sum_{\ell\sim L} b_\ell \lambda_g(\ell)\right|^2 \left|\sum_{n\sim qP} \varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\right|^2 \\ &= c_k \sum_{g\in\mathcal{B}_k(D)} \left|\sum_{n\sim qP} \varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\right|^2 \sum_{\ell_1,\ell_2\sim L} b_{\ell_1}\lambda_g(\ell_1)\overline{b_{\ell_2}}\lambda_g(\ell_2) \end{aligned}$$

and hence we can split up $M(L;k)$ into a diagonal and a non-diagonal term, i.e.,

$$M(L;k) = M^{\Delta}(L;k) + M^{\not\Delta}(L;k)$$

where

$$\begin{aligned} M^{\Delta}(L;k) &= c_k \sum_{g\in\mathcal{B}_k(D)} \left|\sum_{n\sim qP} \varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\right|^2 \sum_{\ell\sim L} |b_\ell|^2 \,|\lambda_g(\ell)|^2 \\ M^{\not\Delta}(L;k) &= c_k \sum_{g\in\mathcal{B}_k(D)} \left|\sum_{n\sim qP} \varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\right|^2 \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\lambda_g(\ell_1)\overline{b_{\ell_2}}\lambda_g(\ell_2). \end{aligned}$$

Similarly, expanding $M(L)$ using Definition 3.1.2 and Definition 2.1.2 yields

$$M(L) = M^{\mathrm{Hol}}(L) + M^{\mathrm{Maa}}(L) + M^{\mathrm{Eis}}(L)$$

where

$$\begin{aligned} M^{\mathrm{Hol}}(L) &= \sum_{\substack{k>0\\ k \text{ even}}} \sum_{g\in\mathcal{B}_k(D)} \dot{\phi}_{a,b}(k)\frac{(k-1)!}{\pi(4\pi)^{k-1}} \left|\sum_{n\sim qP} \varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\right|^2 \sum_{\ell_1,\ell_2\sim L} b_{\ell_1}\lambda_g(\ell_1)\overline{b_{\ell_2}}\lambda_g(\ell_2) \\ M^{\mathrm{Maa}}(L) &= \sum_{g\in\mathcal{B}(D)} \tilde{\phi}(t_g)\frac{4\pi}{\cosh(\pi t_g)} \left|\sum_{n\sim qP} \varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\right|^2 \sum_{\ell_1,\ell_2\sim L} b_{\ell_1}\lambda_g(\ell_1)\overline{b_{\ell_2}}\lambda_g(\ell_2) \\ M^{\mathrm{Eis}}(L) &= \sum_{\chi} \sum_{g\in\mathcal{B}(\chi)} \int_{-\infty}^{\infty} \tilde{\phi}(t)\frac{1}{\cosh(\pi t)} \left|\sum_{n\sim qP} \varrho_g(n,t)K(n)V\Big(\frac{n}{q}\Big)\right|^2 \sum_{\ell_1,\ell_2\sim L} b_{\ell_1}\lambda_\chi(\ell_1,t)\overline{b_{\ell_2}}\lambda_\chi(\ell_2,t)dt. \end{aligned}$$

We can split up $M^{\mathrm{Hol}}(L)$, $M^{\mathrm{Maa}}(L)$ and $M^{\mathrm{Eis}}(L)$ into ***diagonal*** and ***non-diagonal terms***, i.e.,

$$
\begin{aligned}
M^{\mathrm{Hol}}(L) &= M^{\Delta,\mathrm{Hol}}(L) + M^{\not\Delta,\mathrm{Hol}}(L)\\
M^{\mathrm{Maa}}(L) &= M^{\Delta,\mathrm{Maa}}(L) + M^{\not\Delta,\mathrm{Maa}}(L)\\
M^{\mathrm{Eis}}(L) &= M^{\Delta,\mathrm{Eis}}(L) + M^{\not\Delta,\mathrm{Eis}}(L)
\end{aligned}
$$

where

$$
\begin{aligned}
M^{\Delta,\mathrm{Hol}}(L) &= \sum_{\substack{k>0\\ k \text{ even}}} \sum_{g\in\mathcal{B}_k(D)} \dot{\phi}_{a,b}(k)\frac{(k-1)!}{\pi(4\pi)^{k-1}}\Big|\sum_{n\sim qP}\varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\Big|^2 \sum_{\ell\sim L}|b_\ell|^2\,|\lambda_g(\ell)|^2\\
M^{\Delta,\mathrm{Maa}}(L) &= \sum_{g\in\mathcal{B}(D)}\tilde{\phi}(t_g)\frac{4\pi}{\cosh(\pi t_g)}\Big|\sum_{n\sim qP}\varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\Big|^2 \sum_{\ell\sim L}|b_\ell|^2\,|\lambda_g(\ell)|^2\\
M^{\Delta,\mathrm{Eis}}(L) &= \sum_{\chi}\sum_{g\in\mathcal{B}(\chi)}\int_{-\infty}^{\infty}\tilde{\phi}(t)\frac{1}{\cosh(\pi t)}\Big|\sum_{n\sim qP}\varrho_g(n,t)K(n)V\Big(\frac{n}{q}\Big)\Big|^2 \sum_{\ell\sim L}|b_\ell|^2\,|\lambda_\chi(\ell,t)|^2\,dt
\end{aligned}
$$

and

$$
\begin{aligned}
M^{\not\Delta,\mathrm{Hol}}(L) &= \sum_{\substack{k>0\\ k \text{ even}}} \sum_{g\in\mathcal{B}_k(D)} \dot{\phi}_{a,b}(k)\frac{(k-1)!}{\pi(4\pi)^{k-1}}\Big|\sum_{n\sim qP}\varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\Big|^2 \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\lambda_g(\ell_1)\overline{b_{\ell_2}}\lambda_g(\ell_2)\\
M^{\not\Delta,\mathrm{Maa}}(L) &= \sum_{g\in\mathcal{B}(D)}\tilde{\phi}(t_g)\frac{4\pi}{\cosh(\pi t_g)}\Big|\sum_{n\sim qP}\varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\Big|^2 \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\lambda_g(\ell_1)\overline{b_{\ell_2}}\lambda_g(\ell_2)\\
M^{\not\Delta,\mathrm{Eis}}(L) &= \sum_{\chi}\sum_{g\in\mathcal{B}(\chi)}\int_{-\infty}^{\infty}\tilde{\phi}(t)\frac{1}{\cosh(\pi t)}\Big|\sum_{n\sim qP}\varrho_g(n,t)K(n)V\Big(\frac{n}{q}\Big)\Big|^2 \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\lambda_\chi(\ell_1,t)\overline{b_{\ell_2}}\lambda_\chi(\ell_2,t)dt.
\end{aligned}
$$

Similarly, we write

$$M(L) = M^{\Delta}(L) + M^{\not\Delta}(L)$$

where

$$
\begin{aligned}
M^{\Delta}(L) &= M^{\Delta,\mathrm{Hol}}(L) + M^{\Delta,\mathrm{Maa}}(L) + M^{\Delta,\mathrm{Eis}}(L)\\
M^{\not\Delta}(L) &= M^{\not\Delta,\mathrm{Hol}}(L) + M^{\not\Delta,\mathrm{Maa}}(L) + M^{\not\Delta,\mathrm{Eis}}(L).
\end{aligned}
$$

4.1. Estimate of the diagonal terms $M^{\Delta}(L;k)$ and $M^{\Delta}(L)$

Proposition 4.1.1. *Assume that $|K| \le M$. For any $\varepsilon > 0$ we have*

$$M^{\Delta}(L;k) \ll_{\varepsilon,N} qL^{1+\varepsilon}P(P+1)M^2$$

where the implied constant depends only on N and ε.

Proof. Since $|b_\ell| \le 2$, we have for any $g \in \mathcal{B}_k(D)$

$$\sum_{L\le\ell\le 2L}|b_\ell|^2\,|\lambda_g(\ell)|^2 \le 4\sum_{L\le\ell\le 2L}|\lambda_g(\ell)|^2$$

which is by Deligne's bound (Proposition B.0.17)

$$\ll_\varepsilon \sum_{L\le \ell\le 2L} \ell^\varepsilon \ll_\varepsilon L^{1+\varepsilon}.$$

Hence

$$M^{\Delta}(L;k) \ll_\varepsilon c_k L^{1+\varepsilon} \sum_{g\in\mathcal{B}_k(D)} \Big| \sum_{n\sim qP} \varrho_g(n) K(n) V\Big(\frac{n}{q}\Big)\Big|^2$$

and since V satisfies condition $(V(P,Q))$, this is

$$\ll_\varepsilon c_k L^{1+\varepsilon} \sum_{g\in\mathcal{B}_k(D)} \Big| \sum_{n\sim qP} K(n)\varrho_g(n)\Big|^2. \tag{4.1}$$

Hence we get by the large sieve inequality (Theorem B.0.12)

$$M^{\Delta}(L;k) \ll_\varepsilon c_k L^{1+\varepsilon}\Big(1+\frac{qP}{qN}\Big) \sum_{n\sim qP} |K(n)|^2$$

which is

$$\begin{aligned} &\ll_\varepsilon c_k L^{1+\varepsilon}(1+PN^{-1})qPM^2 \\ &\ll_{\varepsilon,N} c_k q L^{1+\varepsilon} P(P+1)M^2. \end{aligned}$$

□

For the other diagonal terms, the analogous result to Proposition 4.1.1 is

Proposition 4.1.2. *Assume that $|K|\le M$. For any $\varepsilon>0$ and $b=\lceil \varepsilon^{-1}\rceil$ we have*

$$M^{\Delta,\mathrm{Hol}}(L),\ M^{\Delta,\mathrm{Maa}}(L),\ M^{\Delta,\mathrm{Eis}}(L) \ll_{\varepsilon,N} qL^{1+\varepsilon}P(P+1)M^2 \tag{4.2}$$

where the implied constant depends only on N and ε.

Proof. The proof is completely analogous to the one of Lemma 5.1 in [22], except that we have to replace p by q. □

Corollary 4.1.3. *We have*

$$M^{\Delta}(L) \ll qL^{1+\varepsilon}P(P+1)M^2.$$

4.2. Estimate of the non-diagonal term $M^{\not\Delta}(L;k)$

Now, we deal with the non-diagonal part, where $\ell_1\ne\ell_2$. We have by Proposition B.0.11 and Proposition B.0.10 that

$$\lambda_g(\ell_1)\lambda_g(\ell_2)\varrho_g(n_1) = \lambda_g(\ell_1\ell_2)\varrho_g(n_1) = \sum_{\substack{d\mid(\ell_1\ell_2,n_1)\\ (d,qN)=1}} \varrho_g\Big(\frac{\ell_1\ell_2 n_1}{d^2}\Big).$$

By this, we get,

$$\begin{aligned}
M^{\not\Delta}(L;k) &= c_k \sum_{g\in\mathcal{B}_k(D)} \Big| \sum_{n\sim qP} \varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\Big|^2 \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\lambda_g(\ell_1)\overline{b_{\ell_2}}\lambda_g(\ell_2) \\
&= c_k \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2\sim qP} K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big) \\
&\qquad\cdot \sum_{g\in\mathcal{B}_k(D)} \lambda_g(\ell_1)\lambda_g(\ell_2)\varrho_g(n_1)\overline{\varrho_g(n_2)} \\
&= c_k \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2\sim qP} \sum_{\substack{d|(\ell_1\ell_2,n_1)\\ (d,qN)=1}} K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big) \\
&\qquad\cdot \sum_{g\in\mathcal{B}_k(D)} \varrho_g\Big(\frac{\ell_1\ell_2 n_1}{d^2}\Big)\overline{\varrho_g(n_2)}.
\end{aligned}$$

By the Petersson formula (Proposition A.0.3), we have that

$$\begin{aligned}
\sum_{g\in\mathcal{B}_k(D)} \varrho_g\Big(\frac{\ell_1\ell_2 n_1}{d^2}\Big)\overline{\varrho_g(n_2)} &= \frac{(4\pi)^{k-1}}{(k-2)!}\Bigg(\delta\Big(\frac{\ell_1\ell_2 n_1}{d^2}, n_2\Big) \\
&\quad + 2\pi i^{-k} \sum_{\substack{c>0\\ D|c}} \frac{1}{c} S\Big(\frac{\ell_1\ell_2 n_1}{d^2}, n_2; c\Big) J_{k-1}\Big(\frac{4\pi\sqrt{\ell_1\ell_2 d^{-2} n_1 n_2}}{c}\Big)\Bigg) \\
&= \frac{1}{\pi c_k}\Bigg(\delta\Big(\frac{\ell_1\ell_2 n_1}{d^2}, n_2\Big) + \Delta_{D,k}\Big(\frac{\ell_1\ell_2 n_1}{d^2}, n_2\Big)\Bigg).
\end{aligned}$$

Thus

$$\begin{aligned}
M^{\not\Delta}(L;k) &= \frac{1}{\pi} \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2\sim qP} \sum_{\substack{d|(\ell_1\ell_2,n_1)\\ (d,qN)=1}} K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big) \\
&\qquad\cdot \Bigg(\delta\Big(\frac{\ell_1\ell_2 n_1}{d^2}, n_2\Big) + \Delta_{D,k}\Big(\frac{\ell_1\ell_2 n_1}{d^2}, n_2\Big)\Bigg) \\
&= M^{\not\Delta,\delta}(L;k) + M^{\not\Delta,\not\delta}(L;k),
\end{aligned}$$

where

$$M^{\not\Delta,\delta}(L;k) = \frac{1}{\pi} \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2\sim qP} \sum_{\substack{d|(\ell_1\ell_2,n_1)\\ (d,qN)=1}} K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big)\delta\Big(\frac{\ell_1\ell_2 n_1}{d^2}, n_2\Big)$$

$$M^{\not\Delta,\not\delta}(L;k) = \frac{1}{\pi} \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2\sim qP} \sum_{\substack{d|(\ell_1\ell_2,n_1)\\ (d,qN)=1}} K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big)\Delta_{D,k}\Big(\frac{\ell_1\ell_2 n_1}{d^2}, n_2\Big).$$

Lemma 4.2.1. *We have*

$$M^{\not\Delta}(L;k) \ll k^3 q^{\frac{1}{2}+\varepsilon} P(P+1)^{1+\varepsilon} Q^4 M^{2\omega(q)} L^3 + k^3 q^{1+\varepsilon} P(P+1) Q^2 M^{2\omega(q)} L.$$

Proof. We will see in Lemma 4.2.2 that

$$M^{\not\Delta,\delta}(L;k) \ll_B qLPM^{2\omega(q)}$$

and in Lemma 4.2.3 that

$$M^{\not\Delta,\not\delta}(L;k) \ll k^3 q^{\frac{1}{2}+11\varepsilon} P^{2+\varepsilon} Q^4 M^{2\omega(q)} L^3 + k^3 q^{1+6\varepsilon} P^2 Q^2 M^{2\omega(q)} L.$$

Hence, we have by renaming ε

$$M^{\not\Delta}(L;k) \ll_{\varepsilon,N} k^3 q^{\frac{1}{2}+\varepsilon} P(P+1)^{1+\varepsilon} Q^4 M^{2\omega(q)} L^3 + k^3 q^{1+\varepsilon} P(P+1) Q^2 M^{2\omega(q)} L.$$

□

4.2.1. Estimate of $M^{\not\Delta,\delta}(L;k)$

Lemma 4.2.2 (Estimate of $M^{\not\Delta,\delta}(L;k)$)**.** *Let $K(n)$ be such that $|K| \leq M$ for some $M \geq 1$ and b_ℓ be such that $|b_\ell| \leq B$ for some $B > 0$. Assume that $qP \geq L$. Then we have*

$$M^{\not\Delta,\delta}(L;k) \ll_B qLPM^2.$$

Proof. We compute

$$\begin{aligned}
M^{\not\Delta,\delta}(L;k) &= \frac{1}{\pi} \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2\sim qP} \sum_{\substack{d|(\ell_1\ell_2,n_1)\\ (d,qN)=1}} K(n_1)\overline{K(n_2)} V\left(\frac{n_1}{q}\right) V\left(\frac{n_2}{q}\right) \delta\Big(\frac{\ell_1\ell_2 n_1}{d^2}, n_2\Big)\\
&= \frac{1}{\pi} \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1\sim qP} \sum_{\substack{d|(\ell_1\ell_2,n_1)\\ (d,qN)=1\\ \frac{\ell_1\ell_2 n_1}{d^2}\sim qP}} K(n_1)\overline{K\left(\frac{\ell_1\ell_2 n_1}{d^2}\right)} V\left(\frac{n_1}{q}\right) V\left(\frac{\ell_1\ell_2 n_1}{d^2 q}\right)\\
&= \frac{1}{\pi} \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{de=\ell_1\ell_2\\ (d,qN)=1}} \sum_{\substack{n_1\sim qP\\ d|n_1\\ \frac{en_1}{d}\sim qP}} K(n_1)\overline{K\left(\frac{en_1}{d}\right)} V\left(\frac{n_1}{q}\right) V\left(\frac{en_1}{dq}\right)
\end{aligned}$$

which is by setting $m = n_1 d^{-1}$ equal to

$$= \frac{1}{\pi} \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{de=\ell_1\ell_2\\ (d,qN)=1}} \sum_{\substack{m\\ m\sim\frac{qP}{d}\\ m\sim\frac{qP}{e}}} K(dm)\overline{K(em)} V\left(\frac{dm}{q}\right) V\left(\frac{em}{q}\right).$$

Hence

$$\left|M^{\not\Delta,\delta}(L;k)\right| \leq \frac{1}{\pi} \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} |b_{\ell_1}|\left|\overline{b_{\ell_2}}\right| \sum_{\substack{de=\ell_1\ell_2\\ (d,qN)=1}} \sum_{\substack{m\\ m\sim\frac{qP}{d}\\ m\sim\frac{qP}{e}}} M^2$$

$$\leq \frac{1}{\pi} \sum_{\substack{\ell_1,\ell_2\sim L \\ \ell_1\neq\ell_2}} |b_{\ell_1}| \left|\overline{b_{\ell_2}}\right| \sum_{\substack{de=\ell_1\ell_2 \\ (d,qN)=1}} M^2 \min\left(\frac{qP}{d}, \frac{qP}{e}\right).$$

Since $de = \ell_1\ell_2$ with $\ell_i \sim L$, we have that $\max(d,e) \geq L$ and hence

$$\begin{aligned} &\leq \frac{4}{\pi} \sum_{\substack{\ell_1,\ell_2\sim L \\ \ell_1\neq\ell_2}} |b_{\ell_1}| \left|\overline{b_{\ell_2}}\right| M^2 qPL^{-1} \\ &\leq \frac{4}{\pi} L^2B^2M^2qPL^{-1} = \frac{4}{\pi}B^2qLPM^2 \\ &\ll_B qLPM^2. \end{aligned}$$

This completes the proof. □

4.2.2. Estimate of $M^{\not\Delta,\not\partial}(L;k)$

Lemma 4.2.3. *We have that*

$$M^{\not\Delta,\not\partial}(L;k) \ll k^3 q^{\frac{1}{2}+11\varepsilon} P^{2+\varepsilon} Q^4 M^{2\omega(q)} L^3 + k^3 q^{1+6\varepsilon} P^2 Q^2 M^{2\omega(q)} L.$$

To prove this Lemma, we define

$$\begin{aligned} M[\phi] &= \sum_{\substack{\ell_1,\ell_2\sim L \\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{d|\ell_1\ell_2 \\ (d,qN)=1}} \sum_{\substack{n_1,n_2 \\ d|n_1}} K(n_1)\overline{K(n_2)} V\left(\frac{n_1}{q}\right) V\left(\frac{n_2}{q}\right) \\ &\quad \cdot \sum_{\substack{c>0 \\ D|c}} \frac{1}{c} S\left(\frac{\ell_1\ell_2 n_1}{d^2}, n_2; c\right) \phi\left(\frac{4\pi}{c}\sqrt{\frac{\ell_1\ell_2n_1n_2}{d^2}}\right) \qquad (4.3) \\ &= \frac{1}{D} \sum_{\substack{\ell_1,\ell_2\sim L \\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{d|\ell_1\ell_2 \\ (d,qN)=1}} \sum_{\substack{n_1,n_2 \\ d|n_1}} K(n_1)\overline{K(n_2)} V\left(\frac{n_1}{q}\right) V\left(\frac{n_2}{q}\right) \\ &\quad \cdot \sum_{c\geq 1} \frac{1}{c} S\left(\frac{\ell_1\ell_2 n_1}{d^2}, n_2; cD\right) \phi\left(\frac{4\pi}{cD}\sqrt{\frac{\ell_1\ell_2n_1n_2}{d^2}}\right) \end{aligned}$$

for an arbitrary function ϕ. Then we have

$$M^{\not\Delta,\not\partial}(L;k) = M[\phi_k]$$

with

$$\phi_k = 2i^{-k} J_{k-1}.$$

Proof of Lemma 4.2.3. We have by Proposition 5.0.1 below that

$$M^{\not\Delta,\not\partial}(L;k) = M[\phi_k] \ll k^3 q^{\frac{1}{2}+11\varepsilon} P^{2+\varepsilon} Q^4 M^{2\omega(q)} L^3 + k^3 q^{1+6\varepsilon} P^2 Q^2 M^{2\omega(q)} L.$$

□

4.3. Estimate of the non-diagonal term $M^{\not\Delta}(L)$

By using Proposition B.0.10 and Proposition B.0.11, we get that

$$\lambda_g(\ell_1)\lambda_g(\ell_2)\varrho_g(n_1) = \lambda_g(\ell_1\ell_2)\varrho_g(n_1) = \sum_{\substack{d|(\ell_1\ell_2,n_1)\\(d,qN)=1}} \varrho_g\Big(\frac{\ell_1\ell_2 n_1}{d^2}\Big).$$

Consequently, we have for the holomorphic part

$$\begin{aligned}
M^{\not\Delta,\mathrm{Hol}}(L) &= \sum_{\substack{k>0\\k \text{ even}}} \sum_{g\in\mathcal{B}_k(D)} \dot{\phi}_{a,b}(k)\frac{(k-1)!}{\pi(4\pi)^{k-1}}\Big|\sum_{n\sim qP}\varrho_g(n)K(n)V\Big(\frac{n}{q}\Big)\Big|^2 \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\lambda_g(\ell_1)\overline{b_{\ell_2}}\lambda_g(\ell_2)\\
&= \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2\sim qP} K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big)\\
&\quad\cdot \sum_{\substack{k>0\\k \text{ even}}} \sum_{g\in\mathcal{B}_k(D)} \dot{\phi}_{a,b}(k)\frac{(k-1)!}{\pi(4\pi)^{k-1}}\lambda_g(\ell_1)\lambda_g(\ell_2)\varrho_g(n_1)\overline{\varrho_g(n_2)}\\
&= \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2\sim qP} \sum_{\substack{d|(\ell_1\ell_2,n_1)\\(d,qN)=1}} K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big)\\
&\quad\cdot \sum_{\substack{k>0\\k \text{ even}}} \sum_{g\in\mathcal{B}_k(D)} \dot{\phi}_{a,b}(k)\frac{(k-1)!}{\pi(4\pi)^{k-1}}\varrho_g\Big(\frac{\ell_1\ell_2 n_1}{d^2}\Big)\overline{\varrho_g(n_2)}
\end{aligned}$$

and similarly for the Maass part

$$\begin{aligned}
M^{\not\Delta,\mathrm{Maa}}(L) &= \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2\sim qP} \sum_{\substack{d|(\ell_1\ell_2,n_1)\\(d,qN)=1}} K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big)\\
&\quad\cdot \sum_{g\in\mathcal{B}(D)} \tilde{\phi}(t_g)\frac{4\pi}{\cosh(\pi t_g)}\varrho_g\Big(\frac{\ell_1\ell_2 n_1}{d^2}\Big)\overline{\varrho_g(n_2)}
\end{aligned}$$

as well as for the Eisenstein part

$$\begin{aligned}
M^{\not\Delta,\mathrm{Eis}}(L) &= \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2\sim qP} \sum_{\substack{d|(\ell_1\ell_2,n_1)\\(d,qN)=1}} K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big)\\
&\quad\cdot \sum_{\chi} \sum_{g\in\mathcal{B}(\chi)} \int_{-\infty}^{\infty} \tilde{\phi}(t)\frac{1}{\cosh(\pi t)}\varrho_g\Big(\frac{\ell_1\ell_2 n_2}{d^2},t\Big)\overline{\varrho_g(n_2,t)}dt.
\end{aligned}$$

Therefore, we get

$$\begin{aligned}
M^{\not\Delta}(L) &= \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2\sim qP} \sum_{\substack{d|(\ell_1\ell_2,n_1)\\(d,qN)=1}} K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big)\\
&\quad\cdot \Bigg(\sum_{\substack{k>0\\k \text{ even}}} \sum_{g\in\mathcal{B}_k(D)} \dot{\phi}_{a,b}(k)\frac{(k-1)!}{\pi(4\pi)^{k-1}}\varrho_g\Big(\frac{\ell_1\ell_2 n_1}{d^2}\Big)\overline{\varrho_g(n_2)}
\end{aligned}$$

$$+\sum_{g\in\mathcal{B}(D)}\tilde{\phi}(t_g)\frac{4\pi}{\cosh(\pi t_g)}\varrho_g\Big(\frac{\ell_1\ell_2 n_1}{d^2}\Big)\overline{\varrho_g(n_2)}$$

$$+\sum_{\chi}\sum_{g\in\mathcal{B}(\chi)}\int_{-\infty}^{\infty}\tilde{\phi}(t)\frac{1}{\cosh(\pi t)}\varrho_g\Big(\frac{\ell_1\ell_2 n_1}{d^2},t\Big)\overline{\varrho_g(n_2,t)}dt\Bigg)$$

$$=\sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}}b_{\ell_1}\overline{b_{\ell_2}}\sum_{n_1,n_2\sim qP}\sum_{\substack{d|(\ell_1\ell_2,n_1)\\(d,qN)=1}}K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big)\Delta_{D,\phi}\Big(n_2,\frac{\ell_1\ell_2 n_1}{d^2}\Big)$$

which is by Kuznetsov's formula (Theorem A.0.7)

$$=\sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}}b_{\ell_1}\overline{b_{\ell_2}}\sum_{n_1,n_2\sim qP}\sum_{\substack{d|(\ell_1\ell_2,n_1)\\(d,qN)=1}}K(n_1)\overline{K(n_2)}V\Big(\frac{n_1}{q}\Big)V\Big(\frac{n_2}{q}\Big)$$

$$\cdot\sum_{\substack{c>0\\ D|c}}\frac{1}{c}S\Big(n_2,\frac{\ell_1\ell_2 n_1}{d^2};c\Big)\phi_{a,b}\Big(\frac{4\pi}{c}\sqrt{\frac{\ell_1\ell_2 n_1 n_2}{d^2}}\Big).$$

Recalling (4.3), the definition of $M[\phi]$, we can write $M^{\not\Delta}(L)$ as

$$M^{\not\Delta}(L)=M[\phi_{a,b}]$$

with

$$\phi_{a,b}(x)=i^{b-a}J_a(x)x^{-b}.$$

Lemma 4.3.1. *We have that*

$$M^{\not\Delta}(L)\ll q^{\frac{1}{2}+11\varepsilon}P^{2+\varepsilon}Q^4M^{2\omega(q)}L^3+q^{1+6\varepsilon}P^2Q^2M^{2\omega(q)}L.$$

Proof. We have by Proposition 5.0.1 below that

$$M^{\not\Delta}(L)=M[\phi_{a,b}]\ll q^{\frac{1}{2}+11\varepsilon}P^{2+\varepsilon}Q^4M^{2\omega(q)}L^3+q^{1+6\varepsilon}P^2Q^2M^{2\omega(q)}L.$$

□

4.4. Completion of the proof of Proposition 3.1.4

By Proposition 4.1.1 and Lemma 4.2.1,

$$M(L;k)=M^{\Delta}(L;k)+M^{\not\Delta}(L;k)\ll k^3(q^{1+\varepsilon}L^{1+\varepsilon}+q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}.$$

Moreover, by Corollary 4.1.3 and Lemma 4.3.1,

$$M(L)=M^{\Delta}(L)+M^{\not\Delta}(L)\ll(q^{1+\varepsilon}L^{1+\varepsilon}+q^{\frac{1}{2}+\varepsilon}L^3Q^2)P(P+1)^{1+\varepsilon}Q^2M^{2\omega(q)}.$$

This completes the proof of Proposition 3.1.4.

5. Estimate of $M[\phi]$ for $\phi = \phi_k$ and $\phi = \phi_{a,b}$

In this section, we examine $M[\phi]$ for an arbitrary function ϕ. We rewrite $M[\phi]$ as

$$M[\phi] = \sum_{\substack{\ell_1,\ell_2\sim L \\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{de=\ell_1\ell_2 \\ (d,qN)=1}} M[\phi; d, e],$$

where

$$M[\phi; d, e] = \frac{1}{qN}\sum_{c\geq 1}\frac{1}{c}\mathcal{E}_\phi(c, d, e)$$

and

$$\begin{aligned}\mathcal{E}_\phi(c, d, e) &= \sum_{n_1}\sum_{n_2} S(en_1, n_2; cqN)K(dn_1)\overline{K(n_2)}\phi\left(\frac{4\pi\sqrt{en_1n_2}}{cqN}\right)V\left(\frac{dn_1}{q}\right)V\left(\frac{n_2}{q}\right) \\ &= \sum_{n_1\geq 1}\sum_{n_2\geq 1} S(en_1, n_2; cqN)K(dn_1)\overline{K(n_2)}H_\phi(n_1, n_2; e) \qquad (5.1)\end{aligned}$$

with

$$H_\phi(x, y; z) = \phi\left(\frac{4\pi\sqrt{zxy}}{cqN}\right)V\left(\frac{dx}{q}\right)V\left(\frac{y}{q}\right).$$

We define a parameter $C = C(d, e) \geq 1$ depending only on d and e. We then decompose

$$M[\phi; d, e] = M^{c>C}[\phi; d, e] + M^{c\leq C}[\phi; d, e]$$

where

$$\begin{aligned}M^{c>C}[\phi; d, e] &= \frac{1}{qN}\sum_{c>C(d,e)}\frac{1}{c}\mathcal{E}_\phi(c, d, e) \\ M^{c\leq C}[\phi; d, e] &= \frac{1}{qN}\sum_{1\leq c\leq C(d,e)}\frac{1}{c}\mathcal{E}_\phi(c, d, e).\end{aligned}$$

Accordingly, we decompose

$$M[\phi] = M^{c>C}[\phi; d, e] + M^{c\leq C}[\phi]$$

where

$$\begin{aligned}M^{c>C}[\phi] &= \sum_{\substack{\ell_1,\ell_2\sim L \\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{de=\ell_1\ell_2 \\ (d,qN)=1}} M^{c>C}[\phi; d, e] \\ M^{c\leq C}[\phi] &= \sum_{\substack{\ell_1,\ell_2\sim L \\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{de=\ell_1\ell_2 \\ (d,qN)=1}} M^{c\leq C}[\phi; d, e].\end{aligned}$$

In what follows, we will choose

$$C = C(d,e) = \max\left(\frac{1}{2}, q^{\varepsilon}P\sqrt{\frac{e}{d}}\right). \tag{5.2}$$

Note that then $C \ll q^{\varepsilon}LP$.

Proposition 5.0.1. *We have*

$$M[\phi_k] \ll k^3 q^{\frac{1}{2}+11\varepsilon}P^{2+\varepsilon}Q^4M^{2\omega(q)}L^3 + k^3q^{1+6\varepsilon}P^2Q^2M^{2\omega(q)}L$$

and

$$M[\phi_{a,b}] \ll q^{\frac{1}{2}+11\varepsilon}P^{2+\varepsilon}Q^4M^{2\omega(q)}L^3 + q^{1+6\varepsilon}P^2Q^2M^{2\omega(q)}L.$$

To give a proof of this proposition, we need estimates for $M^{c>C}[\phi]$ and $M^{c\leq C}[\phi]$. We will give an estimate for $M^{c>C}[\phi]$ in Section 5.1 (Proposition 5.1.1) and an estimate for $M^{c\leq C}[\phi]$ in Section 5.2 (Proposition 5.2.1). With these estimates at our disposal, the proof is very simple.

Proof. Since

$$M[\phi] = M^{c>C}[\phi] + M^{c\leq C}[\phi]$$

and Proposition 5.1.1 tells us that $M^{c>C}[\phi; d, e]$ is negligible, we get by Proposition 5.2.1

$$M[\phi_k] \ll k^3 q^{\frac{1}{2}+11\varepsilon}P^{2+\varepsilon}Q^4M^{2\omega(q)}L^3 + k^3q^{1+6\varepsilon}P^2Q^2M^{2\omega(q)}L$$

and analogously for $M[\phi_{a,b}]$. □

5.1. Estimate of $M^{c>C}[\phi]$

The goal of this section is to prove the following proposition.

Proposition 5.1.1. *Let $\varepsilon > 0$ and d, e be given. Define C as in* (5.2). *Let $k(\varepsilon) = 12\varepsilon^{-1}$. Then*

(i) *for all $k \geq k(\varepsilon)$,*

$$M^{c>C}[\phi_k] \ll q^{-10}L^3M^2P^3,$$

(ii) *for all $a > b > 2$ such that $a - b \geq k(\varepsilon)$,*

$$M^{c>C}[\phi_{a,b}] \ll q^{-10}L^3M^2P^3.$$

5.1.1. Estimate of $\mathcal{E}_{\phi}(c, d, e)$

Lemma 5.1.2. *Let $\phi\colon [0, +\infty[\longrightarrow \mathbb{C}$ be a function such that for some $B \geq 0$, $\kappa \geq 0$ and all $x > 0$*

$$|\phi(x)| \leq Bx^{\kappa}. \tag{5.3}$$

Further, assume that $|K(n)| \leq M$ and that V satisfies condition $(V(Q,P))$. Then

$$\mathcal{E}_{\phi}(c,d,e) \ll_{B,\kappa,N} M^2c^{1-\kappa}\left(\frac{e}{d}\right)^{\frac{\kappa}{2}}q^3P^{2+\kappa}. \tag{5.4}$$

Proof. Using the trivial bound for Kloosterman sums (Proposition A.0.4) and the bound $|K(n)| \leq M$, we get

$$\begin{aligned} |\mathcal{E}_\phi(c,d,e)| &\leq \sum_{n_1}\sum_{n_2} cqNM^2 \, |H_\phi(n_1,n_2;e)| \\ &= cqNM^2 \sum_{n_1}\sum_{n_2} \left|\phi\left(\frac{4\pi\sqrt{en_1n_2}}{cqN}\right)\right| V\left(\frac{dn_1}{q}\right) V\left(\frac{n_2}{q}\right) \end{aligned}$$

and since V satisfies condition ($V(Q,P)$), this is

$$\leq cqNM^2 \sum_{n_1 \sim \frac{qP}{d}} \sum_{n_2 \sim qP} \left|\phi\left(\frac{4\pi\sqrt{en_1n_2}}{cqN}\right)\right|.$$

Furthermore, by (5.3), this becomes

$$\begin{aligned} \mathcal{E}_\phi(c,d,e) &\ll_{B,\kappa,N} (cq)^{1-\kappa} M^2 \sum_{n_1 \sim \frac{qP}{d}} \sum_{n_2 \sim qP} (en_1n_2)^{\frac{\kappa}{2}} \\ &\ll_{B,\kappa,N} (cq)^{1-\kappa} M^2 \left(\frac{e}{d}\right)^{\frac{\kappa}{2}} q^\kappa P^\kappa \sum_{n_1 \sim \frac{qP}{d}} \sum_{n_2 \sim qP} 1 \\ &\ll_{B,\kappa,N} (cq)^{1-\kappa} M^2 \left(\frac{e}{d}\right)^{\frac{\kappa}{2}} q^\kappa P^\kappa q^2 P^2 \frac{1}{d} \end{aligned}$$

which is

$$\ll_{B,\kappa,N} M^2 c^{1-\kappa} \left(\frac{e}{d}\right)^{\frac{\kappa}{2}} q^3 P^{2+\kappa}.$$

□

5.1.2. Proof of Proposition 5.1.1

Recall that

$$\phi_k(x) = 2i^{-k} J_{k-1}(x). \tag{5.5}$$

and by Definition A.0.8,

$$\phi_{a,b}(x) = i^{b-a} J_a(x) x^{-b}. \tag{5.6}$$

First, we derive the following lemma.

Lemma 5.1.3. *With notation as above, assuming that $|K| \leq M$, $a-b \geq 2$, we have*

$$\begin{aligned} M^{c>C}[\phi_{a,b},d,e] &\ll q^2M^2P^2C\left(\frac{P}{C}\sqrt{\frac{e}{d}}\right)^{a-b} \\ M^{c>C}[\phi_k,d,e] &\ll q^2M^2P^2C\left(\frac{P}{C}\sqrt{\frac{e}{d}}\right)^{k-1} \end{aligned}$$

where $C = C(d,e)$ and the implied constant depends on f.

Proof. Note that for the Bessel function J_{k-1}, we have the upper bound

$$J_{k-1}(x) \ll \min(1, x^{k-1}) \tag{5.7}$$

where the implied constant is absolute [12, Equation 8.402 and 8.411]. Combining (5.6) and (5.7) yields

$$|\phi_{a,b}(x)| \leq B_1 i^{b-a} \min(1, x^a) x^{-b},$$

for some absolute constant B_1. By setting $\kappa = a - b$ this is

$$= B_1 i^{-\kappa} \min(1, x^{\kappa+b}) x^{-b} = B_2 \min(x^{-b}, x^{\kappa}) \leq B_2 x^{\kappa}$$

So, assumption (5.3) is satisfied for $\phi_{a,b}$ and hence by (5.4),

$$\tilde{\mathcal{E}}_{\phi_{a,b}}(c, d, e) \ll_{B_2,\kappa,N} M^2 c^{1-\kappa} \left(\frac{e}{d}\right)^{\frac{\kappa}{2}} q^3 P^{2+\kappa}.$$

Consequently

$$\begin{aligned} M^{c>C}[\phi_{a,b}; d, e] &= \frac{1}{qN} \sum_{c>C} \frac{1}{c} \tilde{\mathcal{E}}_{\phi_{a,b}}(c, d, e) \\ &\ll_{B_2,\kappa,N} \frac{1}{N} M^2 \left(\frac{e}{d}\right)^{\frac{\kappa}{2}} q^2 P^{2+\kappa} \sum_{c>C} c^{-\kappa} \\ &\ll_{B_2,\kappa,N} M^2 \left(\frac{e}{d}\right)^{\frac{\kappa}{2}} q^2 P^{2+\kappa} C^{1-\kappa} \\ &= M^2 q^2 C P^2 \left(\frac{P}{C}\sqrt{\frac{e}{d}}\right)^{\kappa} = M^2 q^2 C P^2 \left(\frac{P}{C}\sqrt{\frac{e}{d}}\right)^{a-b}, \end{aligned}$$

since $\kappa \geq 2$.

For ϕ_k, the procedure is similar. By combining (5.5) and (5.7), we analogously obtain

$$|\phi_k(x)| \leq B x^{k-1} = B x^{\kappa},$$

for some $B \geq 0$, where we put $\kappa = k - 1 \geq 0$. Now, we get analogously

$$M^{c>C}[\phi_k; d, e] \ll M^2 q^2 C P^2 \left(\frac{P}{C}\sqrt{\frac{e}{d}}\right)^{\kappa} = M^2 q^2 C P^2 \left(\frac{P}{C}\sqrt{\frac{e}{d}}\right)^{k-1}.$$

This completes the proof. □

Proof of Propositon 5.1.1. By the definition of $C(d, e)$ and Lemma 5.1.3, we have

$$\begin{aligned} M^{c>C}[\phi_k, d, e] &\ll q^2 M^2 P^2 C \left(\frac{P}{C}\sqrt{\frac{e}{d}}\right)^{k-1} \\ &= q^2 M^2 P^2 C q^{-\varepsilon(k-1)} \ll q^{2-\varepsilon(k-1)} M^2 P^2 q^{\varepsilon} L P \\ &= q^{2-\varepsilon k} M^2 P^3 L \leq q^{-10} L M^2 P^3. \end{aligned}$$

Similarly, we obtain

$$M^{c>C}[\phi_{a-b}, d, e] \ll q^{-10} L M^2 P^3.$$

□

5.2. Estimate of $M^{c\le C}[\phi]$

It remains to estimate $M^{c\le C}[\phi]$. Recall that

$$M^{c\le C}[\phi] = \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\ne\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{de=\ell_1\ell_2\\ (d,qN)=1}} M^{c\le C}[\phi; d, e]$$

with

$$M^{c\le C}[\phi; d, e] = \frac{1}{qN}\sum_{1\le c\le C} c^{-1}\mathcal{E}_\phi(c,d,e),$$

where C is given by (5.2). In particular, we can assume that $C \ge 1$ as otherwise the above sum is zero. Precisely, we are going to prove the following proposition. The proof is carried out at the end of Section 5.4.

Proposition 5.2.1. *Assume that $2q^\varepsilon P < L$. Then we have that*

$$M^{c\le C}[\phi_k] \ll k^3 q^{\frac12+11\varepsilon}P^{2+\varepsilon}Q^4M^2L^3 + k^3q^{1+6\varepsilon}P^2Q^2M^2L$$

and

$$M^{c\le C}[\phi_{a,b}] \ll q^{\frac12+11\varepsilon}P^{2+\varepsilon}Q^4M^2L^3 + q^{1+6\varepsilon}P^2Q^2M^2L.$$

5.3. Transformation of $\mathcal{E}_\phi(c,d,e)$

Definition 5.3.1. For $n_1n_2\equiv e \mod cN$ and $(cN,q)=1$, the integral matrix $\gamma(c,d,e,n_1,n_2)$ defined by

$$\gamma(c,d,e,n_1,n_2) = \begin{pmatrix} n_1 & \frac{n_1n_2-e}{cN}\\ cdN & dn_2\end{pmatrix} \in M_2(\mathbb{Z})\cap \mathrm{GL}_2(\mathbb{Q})$$

is called a ***resonating matrix***.

Remark 5.3.2. Observe that the determinant of $\gamma(c,d,e,n_1,n_2)$ is de.

We will transform each of the sums $\mathcal{E}_\phi(c,d,e)$ so that we can connect them with the correlation sums $\mathcal{C}(K;\gamma)$ for suitable matrices γ. Concretely, we are going to prove the following theorem.

Theorem 5.3.3. *Let q, c, N be a positive integers, let d, e be positive integers such that $(de,q)=1$ and let $n_1,n_2\in\mathbb{Z}$. Then we have*

$$\mathcal{E}_\phi(c,d,e) = \frac1q \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\\ n_1n_2\ne 0\\ n_1n_2\equiv e \mod cN\\ (n_2,cN)=1}} \hat{H}_\phi\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)\mathcal{C}\big(K;\gamma(c,d,e,n_1,n_2)\big).$$

There is a remark in order concerning modular inverses. If a is an integer with $(a,q)=1$, we denote its modular inverse with respect to the modulus q by $\overline{a}$, i.e., $\overline{a}$ is the unique integer in $\{0,1,\dots,q-1\}$ such that $a\overline{a}\equiv 1 \mod q$. Clearly, if $(q,cN)=1$, we have

$$\frac{n_1n_2-e}{cN} \equiv (n_1n_2-e)\overline{cN} \mod q.$$

However, when $(q,cN)\ne 1$, the expression on the right hand side does not make sense anymore, as cN does not posses an inverse modulo q, whereas the expression on the left hand side may still make sense. More precisely, the expression

$$\frac{n_1n_2-e}{cN} \mod q$$

makes sense as long as $n_1n_2 - e$ is divisible by cN. For the matrix $\gamma(c,d,e,n_1,n_2)$ this is the case, whence $\gamma(c,d,e,n_1,n_2) \in M_2(\mathbb{Z})$ and a reduction modulo every q makes sense.

The subsequent proof of Theorem 5.3.3 which is a squarefree version of Equation (5.16) in [22] is the first place in this thesis where the proof differs significantly from the one given in [22]. So far, we almost always dealt with q as an "analytic variable" and thus the proofs from the prime case carried over without much difficulty. However, the proof of Theorem 5.3.3 as well as the proofs of many subsequent Theorems makes use of algebraic properties of q and hence it can not be expected that the same proofs which worked in the case of q being prime will also work in the case of q being only squarefree. In particular, to derivation of Equation (5.16) in [22] starts with using the twisted multiplicativity of Kloosterman sums which leads there to Equation (5.12). However, in the case of q squarefree, this does not work anymore and therefore in the subsequent proof we circumvent the use of the twisted multiplicativity of Kloosterman sums.

Proof of Theorem 5.3.3. Recall that $\mathcal{E}_\phi(c,d,e)$ is defined in (5.1). Therefore

$$\begin{aligned}
\mathcal{E}_\phi(c,d,e) &= \sum_{n_1\geq 1}\sum_{n_2\geq 1} S(en_1,n_2;cqN)K(dn_1)\overline{K(n_2)}H_\phi(n_1,n_2;e)\\
&= \sum_{0\leq x_1<cqN}\sum_{0\leq x_2<cqN}\sum_{y_1\in\mathbb{Z}}\sum_{y_2\in\mathbb{Z}} S\big(e(y_1cqN+x_1), y_2cqN+x_2;cqN\big)\\
&\quad\cdot K(d(y_1cqN+x_1))\overline{K(y_2cqN+x_2)}H_\phi(y_1cqN+x_1,y_2cqN+x_2;e)\\
&= \sum_{0\leq x_1<cqN}\sum_{0\leq x_2<cqN} S(ex_1,x_2;cqN)K(dx_1)\overline{K(x_2)}\\
&\quad\cdot \sum_{y_1\in\mathbb{Z}}\sum_{y_2\in\mathbb{Z}} H_\phi\big((y_1,y_2)cqN+(x_1,x_2);e\big)
\end{aligned}$$

which is by the Poisson summation formula (Theorem B.0.20)

$$\begin{aligned}
&= \frac{1}{(cqN)^2}\sum_{0\leq x_1<cqN}\sum_{0\leq x_2<cqN} S(ex_1,x_2;cqN)K(dx_1)\overline{K(x_2)}\\
&\quad\cdot\sum_{n_1\in\mathbb{Z}}\sum_{n_2\in\mathbb{Z}}\hat{H}_\phi\Big(\frac{n_1}{cqN},\frac{n_2}{cqN};e\Big)e\Big(\frac{x_1n_1+x_2n_2}{cqN}\Big)\\
&= \frac{1}{(cqN)^2}\sum_{n_1\in\mathbb{Z}}\sum_{n_2\in\mathbb{Z}}\hat{H}_\phi\Big(\frac{n_1}{cqN},\frac{n_2}{cqN};e\Big)\\
&\quad\cdot\sum_{0\leq x_1<cqN}\sum_{0\leq x_2<cqN} K(dx_1)\overline{K(x_2)}S(ex_1,x_2;cqN)e\Big(\frac{x_1n_1+x_2n_2}{cqN}\Big).
\end{aligned}$$

Furthermore, we have

$$\begin{aligned}
&\sum_{0\leq x_1,x_2<cqN} K(dx_1)\overline{K(x_2)}S(ex_1,x_2;cqN)e\left(\frac{x_1n_1+x_2n_2}{cqN}\right)\\
&\qquad= \sum_{0\leq v_1,v_2<q} K(dv_1)\overline{K(v_2)}\sum_{0\leq u_1,u_2<cN} S\big(e(u_1q+v_1),u_2q+v_2;cqN\big)\\
&\qquad\quad\cdot e\left(\frac{(u_1q+v_1)n_1+(u_2q+v_2)n_2}{cqN}\right)
\end{aligned}$$

$$= \sum_{0\le v_1,v_2<q} K(dv_1)\overline{K(v_2)} \sum_{0\le u_1,u_2<cN} \sum_{\substack{0\le z<cqN\\(z,cqN)=1}} e\left(\frac{e(u_1q+v_1)z+(u_2q+v_2)\overline{z}}{cqN}\right)$$
$$\cdot\, e\left(\frac{(u_1q+v_1)n_1+(u_2q+v_2)n_2}{cqN}\right)$$
$$= \sum_{0\le v_1,v_2<q} K(dv_1)\overline{K(v_2)} \sum_{\substack{0\le z<cqN\\(z,cqN)=1}} e\left(\frac{(ez+n_1)v_1}{cqN}\right) e\left(\frac{(\overline{z}+n_2)v_2}{cqN}\right)$$
$$\cdot \sum_{0\le u_1<cN} e\left(\frac{(eqz+n_1q)u_1}{cqN}\right) \sum_{0\le u_2<cN} e\left(\frac{(q\overline{z}+qn_2)u_2}{cqN}\right)$$
$$= \sum_{0\le v_1,v_2<q} K(dv_1)\overline{K(v_2)} \sum_{\substack{0\le z<cqN\\(z,cqN)=1}} e\left(\frac{(ez+n_1)v_1}{cqN}\right) e\left(\frac{(\overline{z}+n_2)v_2}{cqN}\right)$$
$$\cdot \sum_{0\le u_1<cN} e\left(\frac{(ez+n_1)u_1}{cN}\right) \sum_{0\le u_2<cN} e\left(\frac{(\overline{z}+n_2)u_2}{cN}\right)$$
$$= (cN)^2 \sum_{0\le v_1,v_2<q} K(dv_1)\overline{K(v_2)} \sum_{\substack{0\le z<cqN\\(z,cqN)=1\\ez+n_1\equiv 0 \mod cN\\ \overline{z}+n_2\equiv 0 \mod cN}} e\left(\frac{(ez+n_1)v_1}{cqN}\right) e\left(\frac{(\overline{z}+n_2)v_2}{cqN}\right)$$

and since $(d,q)=1$, this is (note that here, $\overline{d}$ is only modulo q and not modulo cqN)

$$= (cN)^2 \sum_{0\le v_1,v_2<q} K(v_1)\overline{K(v_2)} \sum_{\substack{0\le z<cqN\\(z,cqN)=1\\ez+n_1\equiv 0 \mod cN\\ \overline{z}+n_2\equiv 0 \mod cN}} e\left(\frac{(ez+n_1)\overline{d}v_1}{cqN}\right) \overline{e\left(\frac{-(\overline{z}+n_2)v_2}{cqN}\right)}$$
$$= \begin{cases} (cN)^2 \displaystyle\sum_{0\le v_1,v_2<q} K(v_1)\overline{K(v_2)} \\ \displaystyle\sum_{\substack{0\le z<cqN\\(z,cqN)=1\\ \overline{z}+n_2\equiv 0 \mod cN}} e\left(\frac{(ez+n_1)\overline{d}v_1}{cqN}\right) \overline{e\left(\frac{-(\overline{z}+n_2)v_2}{cqN}\right)} & \text{if } (n_2,cN)=1 \text{ and } e\equiv n_1n_2 \mod cN, \\ 0 & \text{otherwise.} \end{cases}$$

because

$$ez+n_1\equiv 0 \mod cN \qquad \overline{z}+n_2\equiv 0 \mod cN$$

is equivalent to $(n_2,cN)=1$ and

$$e\equiv n_1n_2 \mod cN \qquad \overline{z}+n_2\equiv 0 \mod cN.$$

Thus, we assume that $(n_2,cN)=1$ and $e\equiv n_1n_2 \mod cN$. We define

$$\mathcal{Z} = \left\{z\in(\mathbb{Z}/cqN\mathbb{Z})^\times \,\middle|\, \overline{z}+n_2\equiv 0 \mod cN\right\}$$

and

$$\mathcal{W} = \left\{ w \in \mathbb{Z}/q\mathbb{Z} \,\middle|\, wcN + n_2 \in (\mathbb{Z}/q\mathbb{Z})^\times \right\}.$$

We claim that the map $f\colon \mathcal{Z} \longrightarrow \mathcal{W}$, given by

$$f(z) = \frac{-\overline{z} - n_2}{cN}$$

is a bijection with inverse

$$f^{-1}(w) = \overline{(-wcN - n_2)},$$

where the modular inverse is computed modulo cqN. First note, that since $\overline{z}+n_2 \equiv 0 \mod cN$, we know that

$$w = \frac{-\overline{z} - n_2}{cN} \in \mathbb{Z}.$$

and since $z \in (\mathbb{Z}/cqN\mathbb{Z})^\times$, we get that

$$f(z)cN + n_2 = -\frac{\overline{z} + n_2}{cN} cN + n_2 = -\overline{z} \in (\mathbb{Z}/cqN\mathbb{Z})^\times.$$

Hence the map f is well-defined. Since $wcN + n_2 \in (\mathbb{Z}/cqN\mathbb{Z})^\times$, it is clear that $f^{-1}(w) \in (\mathbb{Z}/cqN\mathbb{Z})^\times$ and since

$$\overline{f^{-1}(w)} + n_2 \equiv -wcN - n_2 + n_2 \equiv -wcN \mod cqN$$

we get that $\overline{f^{-1}(w)} + n_2 \equiv 0 \mod cN$. Thus the map f^{-1} is well-defined. One also easily checks that $f^{-1}\big(f(z)\big) = z$ and $f\big(f^{-1}(w)\big) = w$, which shows that f is a bijection.

By this bijection, we see that for $(n_2, cN) = 1$ and $e \equiv n_1 n_2 \mod cN$,

$$\sum_{\substack{0 \le z < cqN \\ (z,cqN)=1 \\ \overline{z}+n_2 \equiv 0 \mod cN}} e\left(\frac{(ez+n_1)\overline{d}v_1}{cqN}\right) \overline{e\left(\frac{-(\overline{z}+n_2)v_2}{cqN}\right)} = \sum_{\substack{0 \le w < q \\ wcdN - dn_2 \in (\mathbb{Z}/q\mathbb{Z})^\times}} e\Big(\frac{\tilde{w}v_1}{q}\Big) \overline{e\Big(\frac{wv_2}{q}\Big)}$$

where $\tilde{w} = \frac{(ef^{-1}(w)+n_1)\overline{d}}{cN}$. We hence would like to express $\tilde{w}$ in terms of w (modulo q). Since

$$w \equiv -\frac{\overline{z} + n_2}{cN} \mod q$$
$$\tilde{w} \equiv \frac{(ez+n_1)\overline{d}}{cN} \mod q$$

we get that

$$wcNz + n_2 z \equiv -1 \mod qcN$$
$$ez \equiv \tilde{w}cNd - n_1 \mod qcN$$

and hence

$$ze(wcN + n_2) \equiv -e \mod qcN$$
$$ze(wcN + n_2) \equiv (d\tilde{w}cN - n_1)(wcN + n_2) \mod qcN.$$

Hence

$$d\tilde{w}wc^2N^2 + d\tilde{w}n_2cN - n_1wcN - n_1n_2 + e \equiv 0 \mod qcN$$

and since $e - n_1n_2 \equiv 0 \mod cN$, we get

$$\tilde{w}(wcdN + dn_2) \equiv n_1 w + \frac{n_1n_2 - e}{cN} \mod q.$$

So,

$$\tilde{w} \equiv \gamma \cdot w \mod q$$

where

$$\gamma = \begin{pmatrix} n_1 & \frac{n_1n_2-e}{cN} \\ cdN & dn_2 \end{pmatrix}.$$

With this, we can continue the computation from above and get

$$\begin{aligned}
&\sum_{0\leq x_1,x_2<cqN} K(dx_1)\overline{K(x_2)}S(ex_1,x_2;cqN)e\left(\frac{x_1n_1+x_2n_2}{cqN}\right) \\
&= (cN)^2 \sum_{0\leq v_1,v_2<q} K(v_1)\overline{K(v_2)} \sum_{\substack{0\leq w<q \\ wcdN-dn_2\in(\mathbb{Z}/q\mathbb{Z})^\times}} e\Big(\frac{(\gamma\cdot w)v_1}{q}\Big)\overline{e\Big(\frac{wv_2}{q}\Big)} \\
&= q(cN)^2 \sum_{\substack{0\leq w<q \\ wcdN-dn_2\in(\mathbb{Z}/q\mathbb{Z})^\times}} \left(\frac{1}{\sqrt{q}}\sum_{0\leq v_1<q} K(v_1)e\Big(\frac{(\gamma\cdot w)v_1}{q}\Big)\right)\left(\overline{\frac{1}{\sqrt{q}}\sum_{0\leq v_2<q} K(v_2)e\Big(\frac{wv_2}{q}\Big)}\right) \\
&= q(cN)^2 \sum_{\substack{0\leq w<q \\ wcdN-dn_2\in(\mathbb{Z}/q\mathbb{Z})^\times}} \hat{K}(\gamma\cdot w)\overline{\hat{K}(w)} \\
&= q(cN)^2\mathcal{C}(K;\gamma).
\end{aligned}$$

So, we finally obtain

$$\mathcal{E}_\phi(c,d,e) = \frac{1}{q} \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2 \\ n_1n_2\equiv e \mod cN \\ (n_2,cN)=1}} \hat{H}_\phi\left(\frac{n_1}{cqN},\frac{n_2}{cqN};e\right)\mathcal{C}\big(K;\gamma(c,d,e,n_1,n_2)\big).$$

To prove Theorem 5.3.3, it remains to show that we also can include the condition $n_1n_2 \neq 0$. Since $n_1n_2 \equiv e \mod cN$, we also have that $n_1n_2 \equiv e \mod N$. Suppose $n_1n_2 = 0$. Then $e \equiv 0 \mod N$, i.e., $N \mid e$ which is not possible. So we are done. □

5.4. Decomposition of $M^{c\leq C}[\phi]$

Recall that

$$M^{c\leq C}[\phi;d,e] = \frac{1}{qN}\sum_{1\leq c\leq C} c^{-1}\mathcal{E}_\phi(c,d,e)$$

where $C = C(d,e)$ is given by (5.2) and

$$\mathcal{E}_\phi(c,d,e) = \frac{1}{q} \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2 \\ n_1n_2\neq 0 \\ n_1n_2\equiv e \mod cN \\ (n_2,cN)=1}} \hat{H}_\phi\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)\mathcal{C}\big(K;\gamma(c,d,e,n_1,n_2)\big).$$

by Theorem 5.3.3. For positive numbers N_1 and N_2, we consider the square

$$\square = [-N_1, N_1] \times [-N_2, N_2] \subset \mathbb{R}^2. \tag{5.8}$$

We then split up $\mathcal{E}_\phi(c,d,e)$ in a term with $n = (n_1, n_2) \in \square$ (i.e., $|n_1| \leq N_1$ and $|n_2| \leq N_2$) and a term with $n = (n_1, n_2) \notin \square$. Thus, we write

$$\mathcal{E}_\phi(c,d,e) = \mathcal{E}_\phi^{n\in\square}(c,d,e) + \mathcal{E}_\phi^{n\notin\square}(c,d,e),$$

where

$$\mathcal{E}_\phi^{n\in\square}(c,d,e) = \frac{1}{q} \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square \\ n_1n_2\neq 0 \\ n_1n_2\equiv e \mod cN \\ (n_2,cN)=1}} \hat{H}_\phi\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big)\mathcal{C}\big(K;\gamma(c,d,e,n_1,n_2)\big)$$

$$\mathcal{E}_\phi^{n\notin\square}(c,d,e) = \frac{1}{q} \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\setminus\square \\ n_1n_2\neq 0 \\ n_1n_2\equiv e \mod cN \\ (n_2,cN)=1}} \hat{H}_\phi\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big)\mathcal{C}\big(K;\gamma(c,d,e,n_1,n_2)\big).$$

Analogously, we write

$$M^{c\leq C}[\phi;d,e] = M^{c\leq C,n\in\square}[\phi;d,e] + M^{c\leq C,n\notin\square}[\phi;d,e]$$

where

$$M^{c\leq C,n\in\square}[\phi;d,e] = \frac{1}{qN}\sum_{1\leq c\leq C} c^{-1}\mathcal{E}_\phi^{n\in\square}(c,d,e)$$

$$M^{c\leq C,n\notin\square}[\phi;d,e] = \frac{1}{qN}\sum_{1\leq c\leq C} c^{-1}\mathcal{E}_\phi^{n\notin\square}(c,d,e).$$

and

$$M^{c\leq C}[\phi] = M^{c\leq C,n\in\square}[\phi] + M^{c\leq C,n\notin\square}[\phi]$$

where

$$M^{c\leq C,n\in\square}[\phi] = \sum_{\substack{\ell_1,\ell_2\sim L \\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{de=\ell_1\ell_2 \\ (d,qN)=1}} M^{c\leq C,n\in\square}[\phi;d,e]$$

$$M^{c\leq C,n\notin\square}[\phi] = \sum_{\substack{\ell_1,\ell_2\sim L \\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{de=\ell_1\ell_2 \\ (d,qN)=1}} M^{c\leq C,n\notin\square}[\phi;d,e].$$

In what follows, we fix $\varepsilon > 0$ and choose N_1 and N_2 to be

$$N_1 = q^\varepsilon \frac{cd(Q+Z)}{P} \qquad\qquad N_2 = q^\varepsilon \frac{c(Q+Z)}{P}.$$

We proceed as follows. In Section 5.5 we give some general estimates of $\hat{H}_\phi$ which are needed to prove the estimates for $M^{c\leq C,n\in\square}[\phi;d,e]$ in Section 5.7 (Proposition 5.7.1) and for $M^{c\leq C,n\notin\square}[\phi;d,e]$ in Section 5.6 (Proposition 5.6.1). Assuming this results, we can give a proof of Proposition 5.2.1.

Proof of Proposition 5.2.1. Since

$$M^{c\le C}[\phi] = M^{c\le C, n\in\Box}[\phi] + M^{c\le C, n\notin\Box}[\phi]$$

and Proposition 5.6.1 shows that $M^{c\le C, n\notin\Box}[\phi; d, e]$ is negligible compared to $M^{c\le C, n\in\Box}[\phi; d, e]$ we get by Proposition 5.7.1 that

$$M^{c\le C}[\phi_k] \ll M^{c\le C, n\in\Box}[\phi_k] \ll k^3 q^{\frac{1}{2}+11\varepsilon} P^{2+\varepsilon} Q^4 M^{2\omega(q)} L^3 + k^3 q^{1+6\varepsilon} P^2 Q^2 M^{2\omega(q)} L,$$

and that

$$M^{c\le C}[\phi_{a,b}] \ll M^{c\le C, n\in\Box}[\phi_{a,b}] \ll q^{\frac{1}{2}+11\varepsilon} P^{2+\varepsilon} Q^4 M^{2\omega(q)} L^3 + q^{1+6\varepsilon} P^2 Q^2 M^{2\omega(q)} L.$$

□

5.5. Estimates for $\hat{H}_\phi$

In this section, we give estimates for $\hat{H}_\phi$ which are independent of whether $(n_1, n_2) \in \Box$ or not. First of all, we introduce a new parameter:

$$Z = \frac{P}{cN}\sqrt{\frac{e}{d}}. \tag{5.9}$$

Now, we can state the following two lemmas.

Lemma 5.5.1. *Assume that V satisfies $(V(P,Q))$ and that $n_1 n_2 \neq 0$. Then*

(i) *For $\phi = \phi_{a,b}$, we have*

$$\frac{1}{(qN)^2}\hat{H}_{\phi_{a,b}}\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big) \ll \frac{P^2}{d}\frac{Z^{a-b}}{(1+Z)^{a+1/2}}\Big(\frac{cdP^{-1}(Q+Z)}{|n_1|}\Big)^{\mu}\Big(\frac{cP^{-1}(Q+Z)}{|n_2|}\Big)^{\nu}$$

for all μ, $\nu \ge 0$, where the implied constant depends on (N, μ, ν, a, b).

(ii) *For $\phi = \phi_k$, we have*

$$\frac{1}{(qN)^2}\hat{H}_{\phi_k}\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big) \ll \frac{P^2}{d}\Big(\frac{cdP^{-1}(Q+Z)}{|n_1|}\Big)^{\mu}\Big(\frac{cP^{-1}(Q+Z)}{|n_2|}\Big)^{\nu}$$

for all μ, $\nu \ge 0$, where the implied constant depends on (N, μ, ν), but not on k.

Lemma 5.5.2. *Assume that V satisfies $(V(P,Q))$ and that $n_1 n_2 \neq 0$. Then*

(i) *For $\phi = \phi_{a,b}$, we have*

$$\frac{1}{q^2}\hat{H}_{\phi_{a,b}}\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big) \ll q^{\varepsilon}\frac{P^2}{d}\min\Big(\frac{1}{Z^{1/2}}, \frac{Q}{Z}\Big),$$

where the implied constant depends on (a, b, N).

(ii) *For $\phi = \phi_k$, we have*

$$\frac{1}{q^2}\hat{H}_{\phi_k}\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big) \ll k^3 q^{\varepsilon}\frac{P^2}{d}\min\Big(\frac{1}{Z^{1/2}}, \frac{Q}{Z}\Big),$$

where the implied constant depends on N.

Lemma 5.5.1 and Lemma 5.5.2 correspond to Lemma 5.7 and Lemma 5.9 in [22] respectively, where p needs to be replaced by q. Since both lemmas are completely analytic, replacing p by q does not make any difference, as no assumptions on the primality of p are made. Also note that in the statements of Lemma 5.7 and Lemma 5.9 in [22] there is the assumption that (d,e) needs to be of Type (L,L) or of Type $(1,L^2)$. However, this assumption is never used in the proofs and hence can be dropped.

Having this two lemmas at hand, we can continue to estimate $M^{c\leq C}[\phi;d,e]$. We estimate $M^{c\leq C,n\notin\Box}[\phi;d,e]$ in Section 5.6 and $M^{c\leq C,n\in\Box}[\phi;d,e]$ in Section 5.7.

5.6. Estimate of $M^{c\leq C,n\notin\Box}[\phi]$

As it turns out, $M^{c\leq C,n\notin\Box}[\phi]$ is negligible. Precisely, we get:

Proposition 5.6.1 (Estimate of $M^{c\leq C,n\notin\Box}(c,d,e)$)**.** *Let $\varepsilon>0$ and be fixed. Let C be defined by*

$$C=\max\left(\frac{1}{2},p^{\varepsilon}P\sqrt{\frac{e}{d}}\right)$$

and let $\Box$ be given by (5.8)*. Then for $\phi=\phi_{a,b}$ or ϕ_k, we have*

$$M^{c\leq C,n\notin\Box}[\phi]\ll_{\varepsilon,N}L^4P^3M^2(Q+1)^3q^{-1}\ \textit{(negligible)}\ .$$

Proof. By the trivial bound (see (2.1.3))

$$|\mathcal{C}(K;\gamma)|\leq M^2q$$

we get

$$\begin{aligned}
\mathcal{E}_{\phi}^{n\notin\Box}(c,d,e)&=\frac{1}{q}\sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\setminus\Box\\ n_1n_2\neq0\\ n_1n_2\equiv e \mod cN\\ (n_2,cN)=1}}\hat{H}_{\phi}\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)\mathcal{C}\big(K;\gamma(c,d,e,n_1,n_2)\big)\\
&\leq M^2\sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\setminus\Box\\ n_1n_2\neq0\\ n_1n_2\equiv e \mod cN\\ (n_2,cN)=1}}\hat{H}_{\phi}\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)\\
&=M^2\sum_{n_1<-N_1}\sum_{\substack{n_2\\ n_1n_2\neq0\\ n_1n_2\equiv e \mod cN\\ (n_2,cN)=1}}\hat{H}_{\phi}\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)\\
&\quad+M^2\sum_{-N_1\leq n_1\leq N_1}\sum_{\substack{n_2<-N_2\\ n_1n_2\neq0\\ n_1n_2\equiv e \mod cN\\ (n_2,cN)=1}}\hat{H}_{\phi}\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)\\
&\quad+M^2\sum_{-N_1\leq n_1\leq N_1}\sum_{\substack{n_2>N_2\\ n_1n_2\neq0\\ n_1n_2\equiv e \mod cN\\ (n_2,cN)=1}}\hat{H}_{\phi}\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)
\end{aligned}$$

$$+ M^2 \sum_{n_1>N_1} \sum_{\substack{n_2 \\ n_1n_2\neq 0 \\ n_1n_2\equiv e \mod cN \\ (n_2,cN)=1}} \hat{H}_\phi\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big).$$

We now consider this four summands separately. For μ_1, $\nu_1 \geq 0$, we have by Lemma 5.5.1

$$\begin{aligned} M^2 &\sum_{n_1<-N_1} \sum_{\substack{n_2 \\ n_1n_2\neq 0 \\ n_1n_2\equiv e \mod cN \\ (n_2,cN)=1}} \hat{H}_\phi\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big) \\ &\ll M^2q^2N^2\frac{P^2}{d}\big(cdP^{-1}(Q+Z)\big)^{\mu_1}\big(cP^{-1}(Q+Z)\big)^{\nu_1} \sum_{n_1<-N_1} \sum_{\substack{n_2 \\ n_1n_2\neq 0 \\ n_1n_2\equiv e \mod cN \\ (n_2,cN)=1}} \frac{1}{|n_1|^{\mu_1}}\frac{1}{|n_2|^{\nu_1}} \\ &\leq M^2q^2N^2\frac{P^2}{d}\big(cdP^{-1}(Q+Z)\big)^{\mu_1}\big(cP^{-1}(Q+Z)\big)^{\nu_1} \sum_{n_1<-N_1} \sum_{\substack{n_2 \\ n_1n_2\neq 0}} \frac{1}{|n_1|^{\mu_1}}\frac{1}{|n_2|^{\nu_1}}. \end{aligned}$$

By defining $X = cP^{-1}(Q+Z)$ and $Y = M^2q^2N^2\frac{P^2}{d}$, this can be rewritten as

$$= Y(dX)^{\mu_1}X^{\nu_1} \sum_{n_1<-N_1} \sum_{\substack{n_2 \\ n_1n_2\neq 0}} \frac{1}{|n_1|^{\mu_1}}\frac{1}{|n_2|^{\nu_1}}.$$

Analogously, we get

$$M^2 \sum_{n_1>N_1} \sum_{\substack{n_2 \\ n_1n_2\neq 0 \\ n_1n_2\equiv e \mod cN \\ (n_2,cN)=1}} \hat{H}_\phi\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big) \ll Y(dX)^{\mu_1}X^{\nu_1} \sum_{n_1>N_1} \sum_{\substack{n_2 \\ n_1n_2\neq 0}} \frac{1}{|n_1|^{\mu_1}}\frac{1}{|n_2|^{\nu_1}},$$

and for μ_2, $\nu_2 \geq 0$,

$$M^2 \sum_{-N_1\leq n_1\leq N_1} \sum_{\substack{n_2<-N_2 \\ n_1n_2\neq 0 \\ n_1n_2\equiv e \mod cN \\ (n_2,cN)=1}} \hat{H}_\phi\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big) \ll Y(dX)^{\mu_2}X^{\nu_2} \sum_{-N_1\leq n_1\leq N_1} \sum_{\substack{n_2<-N_2 \\ n_1n_2\neq 0}} \frac{1}{|n_1|^{\mu_2}}\frac{1}{|n_2|^{\nu_2}},$$

$$M^2 \sum_{-N_1\leq n_1\leq N_1} \sum_{\substack{n_2>N_2 \\ n_1n_2\neq 0 \\ n_1n_2\equiv e \mod cN \\ (n_2,cN)=1}} \hat{H}_\phi\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big) \ll Y(dX)^{\mu_2}X^{\nu_2} \sum_{-N_1\leq n_1\leq N_1} \sum_{\substack{n_2>N_2 \\ n_1n_2\neq 0}} \frac{1}{|n_1|^{\mu_2}}\frac{1}{|n_2|^{\nu_2}}.$$

Hence, by setting $\nu_1 = 2$, we can compute

$$\begin{aligned} \sum_{n_1<-N_1} \sum_{\substack{n_2 \\ n_1n_2\neq 0}} \frac{1}{|n_1|^{\mu_1}}\frac{1}{|n_2|^2} &= \frac{\pi^2}{3}\sum_{n_1=-\infty}^{-N_1-1} \frac{1}{|n_1|^{\mu_1}} = \frac{\pi^2}{3}\sum_{n_1=N_1+1}^{\infty} \frac{1}{n_1^{\mu_1}} \\ &\leq \frac{\pi^2}{3}\int_{N_1}^{\infty} \frac{1}{n_1^{\mu_1}} dn_1 = \frac{\pi^2}{3}\frac{1}{(\mu_1-1)N_1^{\mu_1-1}}. \end{aligned}$$

Hence,

$$\begin{aligned} Y(dX)^{\mu_1}X^{\nu_1}\sum_{n_1<-N_1}\sum_{\substack{n_2\\ n_1n_2\neq 0}}\frac{1}{|n_1|^{\mu_1}}\frac{1}{|n_2|^{\nu_1}} &\le YX^2\frac{\pi^2}{3}\frac{(dX)^{\mu_1}}{(\mu_1-1)N_1^{\mu_1-1}}\\ &= YX^2\frac{\pi^2}{3}\frac{dX}{(\mu_1-1)q^{\varepsilon(\mu_1-1)}}\\ &= \frac{\pi^2}{3}M^2q^{2-\varepsilon(\mu_1-1)}N^2P^{-1}c^3(Q+Z)^3\frac{1}{\mu_1-1}\end{aligned}$$

which is, by choosing $\mu_1 \ge 3\varepsilon^{-1}+5$,

$$\le \frac{\pi^2}{3}N^2P^{-1}(cQ+LP)^3M^2q^{-1-4\varepsilon}\frac{1}{\mu_1-1}.$$

Because $c\le C = q^{\varepsilon}LP$, this can be rewritten as

$$\begin{aligned} &= \frac{\pi^2}{3}N^2P^{-1}(q^{\varepsilon}QLP+LP)^3M^2q^{-1-4\varepsilon}\frac{1}{\mu_1-1}\\ &\le \frac{8\pi^2}{3}N^2P^{-1}(QLP+LP)^3M^2q^{-1-\varepsilon}\frac{1}{\mu_1-1}\\ &\ll_{\varepsilon,N} L^3P^2M^2(Q+1)^3q^{-1-\varepsilon}.\end{aligned}$$

Analogously, we get

$$Y(dX)^{\mu_1}X^{\nu_1}\sum_{n_1>N_1}\sum_{\substack{n_2\\ n_1n_2\neq 0}}\frac{1}{|n_1|^{\mu_1}}\frac{1}{|n_2|^{\nu_1}} \ll_{\varepsilon,N} L^3P^2M^2(Q+1)^3q^{-1-\varepsilon}.$$

Furthermore, for $\mu_2=0$, we get

$$\begin{aligned} Y(dX)^{\mu_2}X^{\nu_2}\sum_{-N_1\le n_1\le N_1}\sum_{\substack{n_2<-N_2\\ n_1n_2\neq 0}}\frac{1}{|n_1|^{\mu_2}}\frac{1}{|n_2|^{\nu_2}} &= 2N_1YX^{\nu_2}\sum_{n_2=N_2+1}^{\infty}\frac{1}{n_2^{\nu_2}}\\ &\le 2q^{\varepsilon}dXYX^{\nu_2}\frac{1}{(\nu_2-1)N_2^{\nu_2-1}}\\ &= 2q^{\varepsilon}dX^2Y\frac{1}{(\nu_2-1)q^{\varepsilon(\nu_2-1)}}\\ &= 2N^2c^2(Q+Z)^2M^2q^{2+\varepsilon-\varepsilon(\nu_2-1)}\frac{1}{\nu_2-1}\\ &\le 2N^2(cQ+LP)^2M^2q^{2+\varepsilon-\varepsilon(\nu_2-1)}\frac{1}{\nu_2-1}\end{aligned}$$

which is, since $c\le C\le q^{\varepsilon}PL$,

$$\begin{aligned} &\le 2N^2L^2P^2(Q+1)^2M^2q^{2+5\varepsilon-\varepsilon(\nu_2-1)}\frac{1}{\nu_2-1}\\ &\ll_{\varepsilon,N} L^2P^2(Q+1)^2M^2q^{-1},\end{aligned}$$

where we choose $\nu_2 \geq \varepsilon^{-1}3+6$. Combining all this estimates gives

$$\mathcal{E}_\phi^{n\notin\square}(c,d,e) \ll_{\varepsilon,N} L^3P^2M^2(Q+1)^3q^{-1}.$$

Thus, by assuming that $\varepsilon \leq 1$, we get

$$\begin{aligned} M^{c\leq C, n\notin\square}[\phi; d, e] &= \frac{1}{qN}\sum_{1\leq c\leq C} c^{-1}\mathcal{E}_\phi^{n\notin\square}(c,d,e) \\ &\ll_{\varepsilon,N} L^4P^3M^2(Q+1)^3q^{-1} \end{aligned}$$

□

5.7. Estimate of $M^{c\leq C, n\in\square}[\phi]$

The goal of this section is to estimate $M^{c\leq C, n\in\square}[\phi]$. Concretely, we will show the following proposition.

Proposition 5.7.1 (Estimate of $M^{c\leq C, n\in\square}[\phi]$)**.** *Let $q \geq 1$ be a squarefree integer and let $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ be a (q,M)-good q-primeperiodic function. Let $\varepsilon > 0$ be fixed. Let C be defined by*

$$C = \max\Big(\frac{1}{2}, q^\varepsilon P\sqrt{\frac{e}{d}}\Big)$$

and let $\square$ be given by (5.8)*. Then, we have*

$$M^{c\leq C, n\in\square}[\phi_k] \ll k^3q^{\frac{1}{2}+11\varepsilon}P^{2+\varepsilon}Q^4M^{2\omega(q)}L^3 + k^3q^{1+6\varepsilon}P^2Q^2M^{2\omega(q)}L,$$

and

$$M^{c\leq C, n\in\square}[\phi_{a,b}] \ll q^{\frac{1}{2}+11\varepsilon}P^{2+\varepsilon}Q^4M^{2\omega(q)}L^3 + q^{1+6\varepsilon}P^2Q^2M^{2\omega(q)}L.$$

First, note that

$$M^{c\leq C, n\in\square}[\phi] = \sum_{\substack{\ell_1,\ell_2\sim L \\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{de=\ell_1\ell_2 \\ (d,qN)=1}} M^{c\leq C, n\in\square}[\phi; d, e]$$

with

$$M^{c\leq C, n\in\square}[\phi; d, e] = \frac{1}{qN}\sum_{1\leq c\leq C} c^{-1}\mathcal{E}_\phi^{n\in\square}(c,d,e)$$

and that by Theorem 5.3.3, $\mathcal{E}_\phi^{n\in\square}(c,d,e)$ is a sum over products of the form $\hat{H}_\phi(\ldots)\mathcal{C}(K;\gamma)$. Consequently, we derive our estimate by estimating $\hat{H}_\phi$ and $\mathcal{C}(K;\gamma)$ separately. The estimate of $\hat{H}_\phi$ was done in Lemma 5.5.2. However, the estimate of $\mathcal{C}(K;\gamma)$ turns out to be a bit tricky.

More precisely

$$\mathcal{E}_\phi^{n\in\square}(c,d,e) = \frac{1}{q}\sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square \\ n_1n_2\neq 0 \\ n_1n_2\equiv e \mod cN \\ (n_2,cN)=1}} \hat{H}_\phi\Big(\frac{n_1}{cqN}, \frac{n_2}{cqN}\Big)\mathcal{C}\big(K;\gamma(c,d,e,n_1,n_2)\big).$$

with

$$\mathcal{C}(K;\gamma) = \prod_{p\mid q}\mathcal{C}(K_p;\gamma_p).$$

by Proposition 2.2.5, where

$$\gamma_p = \begin{pmatrix} n_1 & \frac{n_1n_2-e}{cN}s_p \\ cdN\overline{s_p} & dn_2 \end{pmatrix} \qquad\qquad s_p \equiv \prod_{\substack{p'\mid q\\ p'\neq p}} \overline{p'} \mod p.$$

We separate the terms in $\mathcal{E}_\phi^{n\in\square}(c,d,e)$ according as to whether

$$\left|\mathcal{C}\big(K_p;\gamma_p(c,d,e,n_1,n_2)\big)\right| \le Mp^{\frac12}. \tag{5.10}$$

When (5.10) fails, γ_p is in the set $\mathbf{G}_{K_p,M}$ of M-correlation matrices (see Definition 2.2.7) and otherwise $\gamma_p \notin \mathbf{G}_{K_p,M}$.

Definition 5.7.2. Fix a squarefree number q. Then we associate to every matrix $\gamma(c,d,e,n_1,n_2)$ its ***type*** $\mathbf{T}[\gamma]$ which is a vector $\mathbf{T}[\gamma] = \big(T[\gamma]_p\big)_{p\mid q}$ given by

$$T[\gamma]_p = \begin{cases} \frac12 & \text{if } \gamma_p \notin \mathbf{G}_{K_p,M}, \\ 1 & \text{if } \gamma_p \in \mathbf{G}_{K_p,M}. \end{cases}$$

Of course, the type depends on q. We denote the space of all possible types by $\mathbf{H} = \left\{\frac12, 1\right\}^{\omega(q)}$, so $|\mathbf{H}| = d(q) \ll q^{\varepsilon}$. For $\mathbf{h}\in\mathbf{H}$, we define

$$q[\mathbf{h}] = \prod_{\substack{p\mid q\\ h_p=1}} p.$$

From the definition of $\mathbf{T}[\gamma]$ we immediately get the following lemma.

Lemma 5.7.3. *If* $\mathbf{T}[\gamma]=\mathbf{h}$ *for some* $\mathbf{h}\in\mathbf{H}$*, then*

$$\left|\mathcal{C}\big(K;\gamma(c,d,e,n_1,n_2)\big)\right| \le \prod_{p\mid q} M^{2h_p}p^{h_p}.$$

We write

$$\mathcal{E}_\phi^{n\in\square}(c,d,e) = \sum_{\mathbf{h}\in\mathbf{H}} \mathcal{E}_\phi^{n\in\square,\mathbf{h}}(c,d,e)$$

where

$$\mathcal{E}_\phi^{n\in\square,\mathbf{h}}(c,d,e) = \frac1q \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq0,\ (n_2,cN)=1\\ n_1n_2\equiv e \mod cN\\ \mathbf{T}[\gamma(c,d,e,n_1,n_2)]=\mathbf{h}}} \hat{H}_\phi\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)\mathcal{C}\big(K;\gamma(c,d,e,n_1,n_2)\big).$$

Similarly, we write

$$M^{c\le C,n\in\square}[\phi] = \sum_{\mathbf{h}\in\mathbf{H}} M^{c\le C,n\in\square,\mathbf{h}}[\phi] \tag{5.11}$$

where

$$M^{c\le C,n\in\square,\mathbf{h}}[\phi] = \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{de=\ell_1\ell_2\\ (d,qN)=1}} M^{c\le C,n\in\square,\mathbf{h}}[\phi;d,e]$$

with

$$M^{c\leq C,n\in\square,\mathbf{h}}[\phi;d,e]=\frac{1}{qN}\sum_{1\leq c\leq C}\frac{1}{c}\mathcal{E}_{\phi}^{n\in\square,\mathbf{h}}(c,d,e).$$

We have the following bound for $M^{c\leq C,n\in\square,\mathbf{h}}[\phi;d,e]$.

Proposition 5.7.4. *Let q be a squarefree integer. Then for any $\varepsilon>0$,*

$$M^{c\leq C,n\in\square,\mathbf{h}}[\phi_k]\ll k^3q^{\frac{1}{2}+10\varepsilon}P^{2+\varepsilon}Q^4M^{2\omega(q)}L^3+k^3q^{1+5\varepsilon}P^2Q^2M^{2\omega(q)}L$$

and

$$M^{c\leq C,n\in\square,\mathbf{h}}[\phi_{a,b}]\ll q^{\frac{1}{2}+10\varepsilon}P^{2+\varepsilon}Q^4M^{2\omega(q)}L^3+q^{1+5\varepsilon}P^2Q^2M^{2\omega(q)}L.$$

We will prove this bound soon, but first we derive Proposition 5.7.1 from it.

Proof of Proposition 5.7.1. By (5.11)

$$M^{c\leq C,n\in\square}[\phi_k]=\sum_{\mathbf{h}\in\mathbf{H}}M^{c\leq C,n\in\square,\mathbf{h}}[\phi]$$

which is by Proposition 5.7.4

$$\begin{aligned}&\ll\sum_{\mathbf{h}\in\mathbf{H}}k^3q^{\frac{1}{2}+10\varepsilon}P^{2+\varepsilon}Q^4M^{2\omega(q)}L^3+\sum_{\mathbf{h}\in\mathbf{H}}k^3q^{1+5\varepsilon}P^2Q^2M^{2\omega(q)}L\\&\ll k^3q^{\frac{1}{2}+11\varepsilon}P^{2+\varepsilon}Q^4M^{2\omega(q)}L^3+k^3q^{1+6\varepsilon}P^2Q^2M^{2\omega(q)}L\end{aligned}$$

and analogously for $M^{c\leq C,n\in\square}[\phi_{a,b};d,e]$. □

5.7.1. Continuation of argument

Definition 5.7.5. For $\mathbf{h}\in\mathbf{H}$ and for a positive integer a, we define

$$a^{\mathbf{h}}=\prod_{\substack{p\mid q\\h_p=1}}(a,p^\infty).$$

Definition 5.7.6. We define

$$\chi_{\mathbf{h}}(c,d,e,n_1,n_2)=\begin{cases}1&\text{if }(n_2,cN)=1,\ n_1n_2\equiv e\pmod{cN}\\&\quad\text{and }T[\gamma(c,d,e,n_1,n_2)]=\mathbf{h},\\0&\text{otherwise.}\end{cases}$$

and

$$S[\mathbf{h}]=\sum_{\substack{\ell_1,\ell_2\sim L\\\ell_1\neq\ell_2}}\sum_{\substack{de=\ell_1\ell_2\\(d,qN)=1}}\sum_{1\leq c\leq C(d,e)}\sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\n_1n_2\neq0}}\chi_{\mathbf{h}}(c,d,e,n_1,n_2).$$

Lemma 5.7.7. *Let q be a squarefree integer and suppose that $(d,q)=1$. Then for every $\mathbf{h}\in\mathbf{H}$ and for any $\varepsilon>0$, we have*

$$M^{c\leq C,n\in\square,\mathbf{h}}[\phi_k]\ll_N k^3q^\varepsilon\frac{PQ}{L}S[\mathbf{h}]\prod_{p\mid q}M^{2h_p}p^{h_p}$$

as well as

$$M^{c\leq C,n\in\square,\mathbf{h}}[\phi_{a,b}]\ll_N q^\varepsilon\frac{PQ}{L}S[\mathbf{h}]\prod_{p\mid q}M^{2h_p}p^{h_p}.$$

Proof. Recall that

$$Z=\frac{P}{cN}\sqrt{\frac{e}{d}}.$$

By Lemma 5.5.2, we have

$$\hat{H}_{\phi_k}\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)\ll_N k^3q^{2+\varepsilon}\frac{P^2Q}{dZ} \tag{5.12}$$

$$\hat{H}_{\phi_{a,b}}\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)\ll_{a,b,N} q^{2+\varepsilon}\frac{P^2Q}{dZ}. \tag{5.13}$$

We compute

$$\begin{aligned}\mathcal{E}^{n\in\square,\mathbf{h}}_{\phi_k}(c,d,e)&=\frac{1}{q}\sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq0,\ (n_2,cN)=1\\ n_1n_2\equiv e \mod cN\\ T[\gamma(c,d,e,n_1,n_2)]=\mathbf{h}}}\hat{H}_{\phi_k}\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)\mathcal{C}\big(K;\gamma(c,d,e,n_1,n_2)\big)\\ &\ll\frac{1}{q}\Big(\prod_{p|q}M^{2h_p}p^{h_p}\Big)\sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq0,\ (n_2,cN)=1\\ n_1n_2\equiv e \mod cN\\ T[\gamma(c,d,e,n_1,n_2)]=\mathbf{h}}}\left|\hat{H}_{\phi_k}\Big(\frac{n_1}{cqN},\frac{n_2}{cqN}\Big)\right|\end{aligned}$$

which is by (5.12)

$$\begin{aligned}&\ll_N k^3q^{1+\varepsilon}\frac{P^2Q}{dZ}\Big(\prod_{p|q}M^{2h_p}p^{h_p}\Big)\sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq0,\ (n_2,cN)=1\\ n_1n_2\equiv e \mod cN\\ T[\gamma(c,d,e,n_1,n_2)]=\mathbf{h}}}1\\ &=k^3q^{1+\varepsilon}\frac{P^2Q}{dZ}\Big(\prod_{p|q}M^{2h_p}p^{h_p}\Big)\sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq0}}\chi_{\mathbf{h}}(c,d,e,n_1,n_2).\end{aligned}$$

Hence

$$\begin{aligned}&M^{c\le C,n\in\square,\mathbf{h}}[\phi_k;d,e]\\ &\qquad=\frac{1}{qN}\sum_{1\le c\le C}\frac{1}{c}\mathcal{E}^{n\in\square,\mathbf{h}}_{\phi_k}(c,d,e)\\ &\qquad\ll q^{\varepsilon}k^3PQ\Big(\prod_{p|q}M^{2h_p}p^{h_p}\Big)\sum_{1\le c\le C}\frac{P}{cdNZ}\sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq0}}\chi_{\mathbf{h}}(c,d,e,n_1,n_2)\end{aligned}$$

which is by the definition of Z

$$=q^{\varepsilon}k^3\frac{PQ}{\sqrt{de}}\Big(\prod_{p|q}M^{2h_p}p^{h_p}\Big)\sum_{1\le c\le C}\sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq0}}\chi_{\mathbf{h}}(c,d,e,n_1,n_2).$$

Therefore

$$\begin{aligned} M^{c\le C,n\in\square,\mathbf{h}}[\phi_k] &= \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} b_{\ell_1}\overline{b_{\ell_2}} \sum_{\substack{de=\ell_1\ell_2\\ (d,qN)=1}} M^{c\le C,n\in\square,\mathbf{h}}[\phi_k;d,e] \\ &\ll \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} \sum_{\substack{de=\ell_1\ell_2\\ (d,qN)=1}} \left|M^{c\le C,n\in\square,\mathbf{h}}[\phi_k;d,e]\right| \\ &\ll q^\varepsilon k^3 PQ\Big(\prod_{p|q} M^{2h_p}p^{h_p}\Big) \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} \sum_{\substack{de=\ell_1\ell_2\\ (d,qN)=1}} \frac{1}{\sqrt{de}} \\ &\quad\cdot \sum_{1\le c\le C} \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq 0}} \chi_{\mathbf{h}}(c,d,e,n_1,n_2) \end{aligned}$$

and since $\sqrt{de}\ge L$, this is

$$\ll q^\varepsilon k^3 \frac{PQ}{L}\Big(\prod_{p|q} M^{2h_p}p^{h_p}\Big) S[\mathbf{h}].$$

Analogously we get the result for $\phi_{a,b}$. □

5.7.2. Estimate of $S[\mathbf{h}]$

Recall that

$$S[\mathbf{h}] = \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} \sum_{\substack{de=\ell_1\ell_2\\ (d,qN)=1}} \sum_{1\le c\le C(d,e)} \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq 0}} \chi_{\mathbf{h}}(c,d,e,n_1,n_2) \tag{5.14}$$

and that we factor the product of distinct primes $\ell_1\ell_2$ (with $\ell_i\sim L$) as $\ell_1\ell_2=de$. Hence we have three types of factorization of completely different nature, which we denote as follows

(i) Type $T(L^2,1)$: this is when $d=\ell_1\ell_2$ and $e=1$, so that $L^2<d\le 4L^2$;
(ii) Type $T(1,L^2)$: this is when $d=1$ and $e=\ell_1\ell_2$, so that $L^2<e\le 4L^2$;
(iii) Type $T(L,L)$: this is when d and e are both $\neq 1$ (so $d=\ell_1$ and $e=\ell_2$ or conversely), so that $L<d\neq e\le 2L$.

Therefore, we split up $S[\mathbf{h}]$ as

$$S[\mathbf{h}] = S^{T(L^2,1)}[\mathbf{h}] + 2S^{T(L,L)}[\mathbf{h}] + S^{T(1,L^2)}[\mathbf{h}],$$

where

$$\begin{aligned} S^{T(L^2,1)}[\mathbf{h}] &= \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2\\ (\ell_1\ell_2,qN)=1}} \sum_{1\le c\le C(\ell_1\ell_2,1)} \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq 0}} \chi_{\mathbf{h}}(c,\ell_1\ell_2,1,n_1,n_2) \\ S^{T(L,L)}[\mathbf{h}] &= \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2\\ (\ell_1,qN)=1}} \sum_{1\le c\le C(\ell_1,\ell_2)} \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq 0}} \chi_{\mathbf{h}}(c,\ell_1,\ell_2,n_1,n_2) \\ S^{T(1,L^2)}[\mathbf{h}] &= \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}} \sum_{1\le c\le C(1,\ell_1\ell_2)} \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\neq 0}} \chi_{\mathbf{h}}(c,1,\ell_1\ell_2,n_1,n_2). \end{aligned}$$

Lemma 5.7.8. *Let $q^\varepsilon P < L$, then*

$$S^{T(L^2,1)}[\mathbf{h}] = 0.$$

Proof. Recall that

$$C = \max\left(\frac{1}{2}, q^\varepsilon P\sqrt{\frac{e}{d}}\right).$$

Hence if (d,e) is of type $T(L^2,1)$, $\sqrt{\frac{d}{e}} \ge L$ and hence

$$C \le \max\left(\frac{1}{2}, \frac{q^\varepsilon P}{L}\right) < 1$$

by the assumption $q^\varepsilon P < L$. Hence the sum over c is empty and thus $S^{T(L^2,1)}[\mathbf{h}] = 0$. □

Hence, for $q^\varepsilon P < L$, we have

$$S[\mathbf{h}] = 2S^{T(L,L)}[\mathbf{h}] + S^{T(1,L^2)}[\mathbf{h}].$$

Definition 5.7.9. For $T(L,L)$, we define

$$\begin{aligned}
\mathcal{C} &= \left\{c \in \mathbb{Z} \,\middle|\, 1 \le c \le \sqrt{2}q^\varepsilon P\right\}\\
\mathcal{D} &= \{d \in \mathbb{Z} \mid L \le d \le 2L,\ d \text{ prime},\ (d,qN) = 1\}\\
\mathcal{N}_2 &= \left\{n_2 \in \mathbb{Z} \,\middle|\, 1 \le |n_2| \le 4q^{2\varepsilon}Q\right\}\\
\mathcal{N}_1 &= \left\{n_1 \in \mathbb{Z} \,\middle|\, 1 \le |n_1| \le 4q^{2\varepsilon}QL\right\}\\
\mathcal{E} &= \{e \in \mathbb{Z} \mid L \le e \le 2L,\ e \text{ prime},\ (e,qN) = 1\}
\end{aligned}$$

and for $T(1,L^2)$, we define

$$\begin{aligned}
\mathcal{C} &= \{c \in \mathbb{Z} \mid 1 \le c \le 2q^\varepsilon PL\}\\
\mathcal{D} &= \{1\}\\
\mathcal{N}_2 &= \left\{n_2 \in \mathbb{Z} \,\middle|\, 1 \le |n_2| \le 4q^{2\varepsilon}QL\right\}\\
\mathcal{N}_1 &= \left\{n_1 \in \mathbb{Z} \,\middle|\, 1 \le |n_1| \le 4q^{2\varepsilon}QL\right\}\\
\mathcal{E} &= \left\{e \in \mathbb{Z} \,\middle|\, 1 \le e \le 4L^2,\ \omega(e) = \Omega(e) = 2,\ (e,qN) = 1\right\}.
\end{aligned}$$

As we will see later, the order in which we are summing over these sets is crucial. Changing the order of summation from equation (5.14) to the one as in Lemma 5.7.10 below massively simplifies the analysis of the resonating matrices in Section 5.8 compared to the analysis done in Section 6 of [22]. This simplification is the basis for generalizing the analysis of resonating matrices to squarefree moduli.

Lemma 5.7.10. *We have*

$$S^{T(L,L)}[\mathbf{h}] \ll \sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{e\in\mathcal{E}}\chi_{\mathbf{h}}(c,d,e,n_1,n_2),$$

and

$$S^{T(1,L^2)}[\mathbf{h}] \ll \sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{e\in\mathcal{E}}\chi_{\mathbf{h}}(c,d,e,n_1,n_2),$$

where the sets $\mathcal{C}$, $\mathcal{D}$, $\mathcal{N}_2$, $\mathcal{N}_1$ and $\mathcal{E}$ are defined as in Definition 5.7.9.

Proof. Since by (5.2)

$$C(d,e) \le q^\varepsilon P\sqrt{\frac{e}{d}}$$

we have that for $\ell_1, \ell_2 \sim L$,

$$C(\ell_1,\ell_2) \le \sqrt{2}q^\varepsilon P$$
$$C(1,\ell_1\ell_2) \le 2q^\varepsilon PL.$$

Note that for (d,e) of type $T(L,L)$,

$$N_1 = q^\varepsilon \frac{cd(Q+Z)}{P} = q^\varepsilon \frac{cd}{P}\left(Q + \frac{P}{cN}\sqrt{\frac{e}{d}}\right) = q^\varepsilon\left(\frac{cdQ}{P} + \frac{\sqrt{ed}}{N}\right) \le 2q^\varepsilon L\left(\frac{cQ}{P} + \frac{1}{N}\right)$$

and since $c \le C \le \sqrt{2}q^\varepsilon P$, this is

$$\le 2q^\varepsilon L\left(\sqrt{2}q^\varepsilon Q + \frac{1}{N}\right) \le 4q^{2\varepsilon}QL,$$

since $q^\varepsilon Q \ge 1$. Furthermore,

$$N_2 = \frac{N_1}{d} \le \frac{N_1}{L} \le 4q^{2\varepsilon}Q.$$

For (d,e) of type $T(1,L^2)$,

$$N_1 = q^\varepsilon \frac{c(Q+Z)}{P} = q^\varepsilon\left(\frac{cQ}{P} + \frac{\sqrt{e}}{N}\right)$$

and since $c \le C \le 2q^\varepsilon PL$, this is

$$\le 2q^\varepsilon L\left(q^\varepsilon Q + \frac{1}{N}\right) \le 4q^{2\varepsilon}QL,$$

and

$$N_2 = N_1 \le 4q^{2\varepsilon}QL.$$

Therefore we can rewrite $S^{T(1,L^2)}[\mathbf{h}]$ as

$$\begin{aligned} S^{T(1,L^2)}[\mathbf{h}] &= \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\ne\ell_2}} \sum_{1\le c\le C(1,\ell_1\ell_2)} \sum_{\substack{(n_1,n_2)\in\mathbb{Z}^2\cap\square\\ n_1n_2\ne 0}} \chi_{\mathbf{h}}(c,1,\ell_1\ell_2,n_1,n_2) \\ &\le \sum_{\substack{L\le\ell_1\le 2L\\ \ell_1 \text{ prime}}} \sum_{\substack{L\le\ell_2\le 2L\\ \ell_2 \text{ prime}\\ \ell_1\ne\ell_2}} \sum_{c\in\mathcal{C}} \sum_{\substack{-N_1\le n_1\le N_1\\ n_1\ne 0}} \sum_{\substack{-N_2\le n_2\le N_2\\ n_2\ne 0}} \chi_{\mathbf{h}}(c,1,\ell_1\ell_2,n_1,n_2) \\ &\le \sum_{\substack{1\le e\le 4L^2\\ \omega(e)=\Omega(e)=2}} d(e) \sum_{c\in\mathcal{C}} \sum_{\substack{-N_1\le n_1\le N_1\\ n_1\ne 0}} \sum_{\substack{-N_2\le n_2\le N_2\\ n_2\ne 0}} \chi_{\mathbf{h}}(c,1,e,n_1,n_2) \end{aligned}$$

where $d(e)$ denotes the number of divisors of e and thus

$$\le 4\sum_{c\in\mathcal{C}} \sum_{\substack{-N_2\le n_2\le N_2\\ n_2\ne 0}} \sum_{\substack{-N_1\le n_1\le N_1\\ n_1\ne 0}} \sum_{\substack{1\le e\le 4L^2\\ \omega(e)=\Omega(e)=2}} \chi_{\mathbf{h}}(c,1,e,n_1,n_2)$$

$$\le 4\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{e\in\mathcal{E}}\chi_{\mathbf{h}}(c,d,e,n_1,n_2).$$

For $S^{T(L,L)}[\mathbf{h}]$ we get

$$\begin{aligned}
S^{T(L,L)}[\mathbf{h}] &= \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}}\sum_{\substack{de=\ell_1\ell_2\\ (d,qN)=1}}\sum_{1\le c\le C(d,e)}\sum_{(n_1,n_2)\in\mathbb{Z}^2\cap\square}\chi_{\mathbf{h}}(c,d,e,n_1,n_2)\\
&\le \sum_{\substack{\ell_1,\ell_2\sim L\\ \ell_1\neq\ell_2}}\sum_{\substack{de=\ell_1\ell_2\\ (d,qN)=1}}\sum_{1\le c\le\tilde{C}}\sum_{-N_1\le n_1\le N_1}\sum_{-N_2\le n_2\le N_2}\chi_{\mathbf{h}}(c,d,e,n_1,n_2)\\
&\le \sum_{L\le\ell_1\le 2L}\sum_{L\le\ell_2\le 2L}\sum_{1\le c\le\tilde{C}}\sum_{-N_1\le n_1\le N_1}\sum_{-N_2\le n_2\le N_2}\chi_{\mathbf{h}}(c,\ell_1,\ell_2,n_1,n_2)\\
&\le \sum_{1\le c\le\tilde{C}}\sum_{L\le d\le 2L}\sum_{-N_1\le n_1\le N_1}\sum_{-N_2\le n_2\le N_2}\sum_{L\le e\le 2L}\chi_{\mathbf{h}}(c,d,e,n_1,n_2)\\
&= \sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{e\in\mathcal{E}}\chi_{\mathbf{h}}(c,d,e,n_1,n_2),
\end{aligned}$$

where $\tilde{C}=\sqrt{2}q^{\varepsilon}P$. □

5.7.3. A simplified version of Proposition 5.7.4

The proof in the general case is quite technical, as for every prime $p|q$, the correlation matrix modulo p may be of a different type, e.g., for one p, γ_p may be parabolic while for some other p, γ_p may be a torus. This is carried out in full detail in Section 5.7.4. Here, we will give the proof of the simple case where all correlation matrices γ_p are identity matrices. This should give a flavour of how the proof in the general case works.

Concretely, we will prove Proposition 5.7.4 in the simplified case where for every $p\mid q$

$$\mathbf{G}_{K_p,M}\subset\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}.$$

As already mentioned in the introduction, even though this is a massive simplification of the problem, there are many applications where already this case is sufficient. For example for a non-trivial additive character ψ of $\mathbb{F}_q$, q prime, the function $K(x)=\psi(\overline{x})$ satisfies $\mathbf{G}_{K_p,M}=\{1\}$ as shown in [22, Section 11.1].

We introduce the set

$$\mathcal{B}=\left\{(c,d,n_2,n_1,e)\in\mathcal{C}\times\mathcal{D}\times\mathcal{N}_2\times\mathcal{N}_1\times\mathcal{E}\;\middle|\;\begin{array}{l}(n_2,cN)=1,\ n_1n_2\equiv e\mod cN\text{ and}\\ \forall p|q[\mathbf{h}]\colon\gamma_p(c,d,e,n_1,n_2)=\begin{pmatrix}1&0\\0&1\end{pmatrix}\end{array}\right\}.$$

Hence

$$\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{e\in\mathcal{E}}\chi_{\mathbf{h}}(c,d,e,n_1,n_2)\le\sum_{i\in\mathcal{I}_{q[\mathbf{h}]}}\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{\substack{e\in\mathcal{E}\\(c,d,n_2,n_1,e)\in\mathcal{B}}}1.$$

and thus

$$S^{T(1,L^2)}[\mathbf{h}]\ll\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{\substack{e\in\mathcal{E}\\(c,d,n_2,n_1,e)\in\mathcal{B}}}1,$$

as well as

$$S^{T(L,L)}[\mathbf{h}] \ll \sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{\substack{e\in\mathcal{E}\\(c,d,n_2,n_1,e)\in\mathcal{B}}} 1.$$

Suppose that $(c,d,n_2,n_1,e)\in\mathcal{B}$. Hence

$$cdN \equiv 0 \mod q[\mathbf{h}]$$

and since $(dN,q)=1$, we get that

$$c \equiv 0 \mod q[\mathbf{h}]. \tag{5.15}$$

First we estimate $S^{T(1,L^2)}[\mathbf{h}]$. Since in this case

$$\mathcal{C} = \{c\in\mathbb{Z}\mid 1\le c\le 2q^{\varepsilon}PL\}$$

we get by equation (5.15) that the $S^{T(1,L^2)}[\mathbf{h}]=0$ if $q[\mathbf{h}]>2q^{\varepsilon}PL$. Hence we can assume that $q[\mathbf{h}]\le 2q^{\varepsilon}PL$. Thus we can estimate

$$\begin{aligned}
S^{T(1,L^2)}[\mathbf{h}] &\ll \sum_{\substack{c\in\mathcal{C}\\ c\equiv 0 \mod q[\mathbf{h}]}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{\substack{e\in\mathcal{E}\\ e\equiv n_1n_2 \mod cN}} 1\\
&\ll \sum_{\substack{c\in\mathcal{C}\\ c\equiv 0 \mod q[\mathbf{h}]}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\left(\frac{\|\mathcal{E}\|}{cN}+1\right)\\
&\ll \sum_{\substack{c\in\mathcal{C}\\ c\equiv 0 \mod q[\mathbf{h}]}}\|\mathcal{D}\|\,\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\left(\frac{\|\mathcal{E}\|}{cN}+1\right)\\
&\ll q^{4\varepsilon}Q^2\left(\sum_{\substack{1\le c\le 2q^{\varepsilon}PL\\ c\equiv 0 \mod q[\mathbf{h}]}}\frac{L^4}{cN}+\sum_{\substack{1\le c\le 2q^{\varepsilon}PL\\ c\equiv 0 \mod q[\mathbf{h}]}}L^2\right)\\
&\ll_N \frac{q^{5\varepsilon}P^{\varepsilon}Q^2L^{4+\varepsilon}}{q[\mathbf{h}]}+\frac{q^{5\varepsilon}PQ^2L^3}{q[\mathbf{h}]}\\
&\ll \frac{q^{5\varepsilon}P^{\varepsilon}Q^2L^{4+\varepsilon}}{q[\mathbf{h}]}.
\end{aligned}$$

Now, we estimate $S^{T(L,L)}[\mathbf{h}]$. Since in this case

$$\mathcal{C} = \left\{c\in\mathbb{Z}\,\middle|\, 1\le c\le \sqrt{2}q^{\varepsilon}P\right\}$$

we get by equation (5.15) that the $S^{T(L,L)}[\mathbf{h}]=0$ if $q[\mathbf{h}]>\sqrt{2}q^{\varepsilon}P$. Hence we can assume that $q[\mathbf{h}]\le\sqrt{2}q^{\varepsilon}P$. Thus we can estimate

$$\begin{aligned}
S^{T(L,L)}[\mathbf{h}] &\ll \sum_{\substack{c\in\mathcal{C}\\ c\equiv 0 \mod q[\mathbf{h}]}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{\substack{e\in\mathcal{E}\\ e\equiv n_1n_2 \mod cN}} 1\\
&\ll \sum_{\substack{c\in\mathcal{C}\\ c\equiv 0 \mod q[\mathbf{h}]}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\left(\frac{\|\mathcal{E}\|}{cN}+1\right)
\end{aligned}$$

$$\begin{aligned}
&\ll \sum_{\substack{c\in\mathcal{C}\\ c\equiv 0 \mod q[\mathbf{h}]}} \|\mathcal{D}\|\,\|\mathcal{N}_2\|\,\|\mathcal{N}_1\| \left(\frac{\|\mathcal{E}\|}{cN}+1\right)\\
&\ll q^{4\varepsilon}Q^2\left(\sum_{\substack{1\le c\le \sqrt{2}q^{\varepsilon}P\\ c\equiv 0 \mod q[\mathbf{h}]}} \frac{L^3}{cN} + \sum_{\substack{1\le c\le \sqrt{2}q^{\varepsilon}P\\ c\equiv 0 \mod q[\mathbf{h}]}} L^2\right)\\
&\ll_N \frac{q^{5\varepsilon}P^{\varepsilon}Q^2L^3}{q[\mathbf{h}]} + \frac{q^{5\varepsilon}PQ^2L^2}{q[\mathbf{h}]}\\
&\ll \frac{q^{5\varepsilon}P^{\varepsilon}Q^2L^3}{q[\mathbf{h}]}.
\end{aligned}$$

Therefore

$$S[\mathbf{h}] = 2S^{T(L,L)}[\mathbf{h}] + S^{T(1,L^2)}[\mathbf{h}] \ll \frac{q^{5\varepsilon}P^{\varepsilon}Q^2L^{4+\varepsilon}}{q[\mathbf{h}]}.$$

Consequently, by Lemma 5.7.7,

$$\begin{aligned}
M^{c\le C, n\in\square,\mathbf{h}}[\phi_k; d, e] &\ll k^3q^{\varepsilon}\frac{PQ}{L}S[\mathbf{h}]\prod_{p|q}M^{2h_p}p^{h_p}\\
&\ll k^3q^{\varepsilon}\frac{PQ}{L}\frac{q^{5\varepsilon}P^{\varepsilon}Q^2L^{4+\varepsilon}}{q[\mathbf{h}]}\prod_{p|q}M^{2h_p}p^{h_p}\\
&\ll k^3q^{\varepsilon}\frac{PQ}{L}\frac{q^{5\varepsilon}P^{\varepsilon}Q^2L^{4+\varepsilon}}{q[\mathbf{h}]^{\frac{1}{2}}}M^{2\omega(q)}q[\mathbf{h}]^{\frac{1}{2}}q^{\frac{1}{2}}
\end{aligned}$$

which is the bound of Proposition 5.7.4 in this simplified case.

5.7.4. Proof of Propsition 5.7.4

Recall Definition 2.2.7. If $T[\gamma] = \mathbf{h}$ and K is (p, M)-good for every prime p, then we have that for every $p \mid q[\mathbf{h}]$,

$$\gamma_p(c, d, e, n_1, n_2) \in \mathcal{A}_p = \bigcup_{i\in\mathcal{I}_p} \mathcal{A}_p^i.$$

By defining

$$\mathcal{I}_{q[\mathbf{h}]} = \prod_{p|q[\mathbf{h}]} \mathcal{I}_p.$$

we get, that if $T[\gamma] = \mathbf{h}$ and K is (p, M)-good for every prime p, then there is some $i \in \mathcal{I}_{q[\mathbf{h}]}$ such that for every $p \mid q[\mathbf{h}]$,

$$\gamma_p(c, d, e, n_1, n_2) \in \mathcal{A}_p^{i_p}.$$

We introduce the short notation $\gamma(c, d, e, n_1, n_2) \in \mathcal{A}^i_{q[\mathbf{h}]}$ for this. In addition, we introduce the set

$$\mathcal{B}_{cN} = \{(c, d, n_2, n_1, e) \in \mathcal{C}\times\mathcal{D}\times\mathcal{N}_2\times\mathcal{N}_1\times\mathcal{E} \mid (n_2, cN) = 1 \text{ and } n_1n_2 \equiv e \mod cN\}.$$

Hence

$$\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{e\in\mathcal{E}}\chi_{\mathbf{h}}(c, d, e, n_1, n_2) \le \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}}\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{n_2\in\mathcal{N}_2}\sum_{n_1\in\mathcal{N}_1}\sum_{\substack{e\in\mathcal{E}\\ (c,d,n_2,n_1,e)\in\mathcal{B}_{cN}\\ \gamma(c,d,e,n_1,n_2)\in\mathcal{A}^i_{q[\mathbf{h}]}}} 1.$$

Thus we get

Lemma 5.7.11. *If K is (p,M)-good for every prime p, then*

$$S^{T(1,L^2)}[\mathbf{h}] \ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{C}} \sum_{d\in\mathcal{D}} \sum_{n_2\in\mathcal{N}_2} \sum_{n_1\in\mathcal{N}_1} \sum_{\substack{e\in\mathcal{E} \\ (c,d,n_2,n_1,e)\in\mathcal{B}_{cN} \\ \gamma(c,d,e,n_1,n_2)\in\mathcal{A}^i_{q[\mathbf{h}]}}} 1,$$

and

$$S^{T(L,L)}[\mathbf{h}] \ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{C}} \sum_{d\in\mathcal{D}} \sum_{n_2\in\mathcal{N}_2} \sum_{n_1\in\mathcal{N}_1} \sum_{\substack{e\in\mathcal{E} \\ (c,d,n_2,n_1,e)\in\mathcal{B}_{cN} \\ \gamma(c,d,e,n_1,n_2)\in\mathcal{A}^i_{q[\mathbf{h}]}}} 1,$$

where $\mathcal{C}$, $\mathcal{D}$, $\mathcal{N}_2$, $\mathcal{N}_1$ and $\mathcal{E}$ are defined as in Definition 5.7.9.

Lemma 5.7.11 indicates, that one difficulties which arises in the general case is, that we have to deal with "mixed cases", e.g., for one prime $p|q[\mathbf{h}]$ dividing γ_p may be parabolic while for some other prime $p|q[\mathbf{h}]$, γ_p is a torus. This is the reason, why we introduced the sum over $\mathcal{I}_{q[\mathbf{h}]}$ in Lemma 5.7.11. Also note that the formulas for $S^{T(1,L^2)}[\mathbf{h}]$ and $S^{T(L,L)}[\mathbf{h}]$ in Lemma 5.7.11 look the same. However, they are not, as the sets $\mathcal{C}$, $\mathcal{D}$, $\mathcal{N}_2$, $\mathcal{N}_1$ and $\mathcal{E}$ are not the same for $T(L,L)$ as for $T(1,L^2)$ (see Definition 5.7.9).

5.7.5. Restriction sets

We start with a definition of the restriction value.

Definition 5.7.12. For a subset

$$\mathcal{R} \subset \mathbb{Z}$$

and some integer $m \geq 1$ we define the ***restriction value of $\mathcal{R}$ modulo m***

$$r_m(\mathcal{R}) = \prod_{p|m} p^{\omega_p}$$

where for every prime $p \mid m$, $\omega_p \in \mathbb{Z}_{\geq 0}$ is the biggest non-negative integer such that $\mathcal{R}$ is contained in a congruence class modulo p^{ω_p}, i.e., such that there exists $y \in \mathbb{Z}$ with

$$\{x \in \mathcal{R} \mid x \equiv y \mod p^{\omega_p}\} = \mathcal{R}.$$

Let us consider some properties of the restriction value. First note that if m and n are two coprime moduli, then

$$r_m(\mathcal{R})r_n(\mathcal{R}) = r_{mn}(\mathcal{R}).$$

Moreover, for a modulus m, by the Chinese remainder theorem, there exists an integer $y \in \mathbb{Z}$ such that for every $x \in \mathcal{R}$,

$$x \equiv y \mod r_m(\mathcal{R}).$$

It also follows directly from the definition, that if $\mathcal{R}_1, \mathcal{R}_2 \subset \mathbb{Z}$ are two subsets of the integers, then for the intersection

$$\mathcal{R} = \mathcal{R}_1 \cap \mathcal{R}_2$$

holds that

$$r_m(\mathcal{R}) \geq \max\{r_m(\mathcal{R}_1), r_m(\mathcal{R}_2)\}.$$

Consequently, for two coprime moduli m_1 and m_2, we have then

$$r_{m_1m_2}(\mathcal{R}) = r_{m_1}(\mathcal{R})r_{m_2}(\mathcal{R}) \ge r_{m_1}(\mathcal{R}_1)r_{m_2}(\mathcal{R}_2).$$

If $\mathcal{S}$ is an interval in $\mathbb{Z}$ and $\mathcal{R} \subset \mathcal{S}$, the size of $\mathcal{R}$ can be bounded by

$$|\mathcal{R}| \le \left\lceil \frac{|\mathcal{S}|}{r_m(R)} \right\rceil \le \frac{|\mathcal{S}|}{r_m(R)} + 1. \tag{5.16}$$

More generally, if $\mathcal{S}$ is some arbitrary subset of $\mathbb{Z}$ and $\mathcal{R} \subset \mathcal{S}$, we can bound the size of $\mathcal{R}$ by

$$|\mathcal{R}| \le \left\lceil \frac{\|\mathcal{S}\|}{r_m(R)} \right\rceil \le \frac{\|\mathcal{S}\|}{r_m(R)} + 1,$$

where $\|\mathcal{S}\| = \max \mathcal{S} - \min \mathcal{S} + 1$. From this it is clear that if we want good bounds on the size of $\mathcal{R}$, it is useful if the restriction value $r_m(R)$ is big. However, this is not the only issue. If the interval $\mathcal{S}$ is short (compared to $r_m(R)$, then the error in (5.16) may be huge compared to $\frac{|\mathcal{S}|}{r_m(R)}$, which is often not desirable. So, we would like to have better estimates in this case.

Definition 5.7.13. Let p be a prime and $i_p \in \mathcal{I}_p$. We call sets $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$ with

$$\begin{aligned}
&\mathcal{R}^c_{p,i_p} \subset \mathcal{C}\\
&\mathcal{R}^d_{p,i_p} \subset \mathcal{R}^c_{p,i_p} \times \mathcal{D} \subset \mathcal{C} \times \mathcal{D}\\
&\mathcal{R}^{n_2}_{p,i_p} \subset \mathcal{R}^d_{p,i_p} \times \mathcal{N}_2 \subset \mathcal{C} \times \mathcal{D} \times \mathcal{N}_2\\
&\mathcal{R}^{n_1}_{p,i_p} \subset \mathcal{R}^{n_2}_{p,i_p} \times \mathcal{N}_1 \subset \mathcal{C} \times \mathcal{D} \times \mathcal{N}_2 \times \mathcal{N}_1\\
&\mathcal{R}^e_{p,i_p} \subset \mathcal{R}^{n_1}_{p,i_p} \times \mathcal{E} \subset \mathcal{C} \times \mathcal{D} \times \mathcal{N}_2 \times \mathcal{N}_1 \times \mathcal{E}
\end{aligned}$$

locally admissible at p, if

$$\gamma_p(c,d,e,n_1,n_2) \in \mathcal{A}_p^{i_p} \quad \text{implies} \quad (c,d,n_1,n_2,e) \in \mathcal{R}^e_{p,i_p}.$$

Additionally, we define

$$\begin{aligned}
\mathcal{R}^d_{p,i_p}[c] &= \left\{ d \in \mathcal{D} \,\middle|\, (c,d) \in \mathcal{R}^c_{p,i_p} \right\} \subset \mathcal{D}\\
\mathcal{R}^{n_2}_{p,i_p}[c,d] &= \left\{ n_2 \in \mathcal{N}_2 \,\middle|\, (c,d,n_2) \in \mathcal{R}^{n_2}_{p,i_p} \right\} \subset \mathcal{N}_2\\
\mathcal{R}^{n_1}_{p,i_p}[c,d,n_2] &= \left\{ n_1 \in \mathcal{N}_1 \,\middle|\, (c,d,n_2,n_1) \in \mathcal{R}^{n_1}_{p,i_p} \right\} \subset \mathcal{N}_1\\
\mathcal{R}^e_{p,i_p}[c,d,n_2,n_1] &= \left\{ e \in \mathcal{E} \,\middle|\, (c,d,n_2,n_1,e) \in \mathcal{R}^e_{p,i_p} \right\} \subset \mathcal{E}.
\end{aligned}$$

Furthermore, for $i \in \mathcal{I}_{q[\mathbf{h}]}$, we call $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})_{p|q[\mathbf{h}]}$ ***admissible***, if for every p dividing $q[\mathbf{h}]$, $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$ is locally admissible at p.

Definition 5.7.14. Let $i \in \mathcal{I}_{q[\mathbf{h}]}$ and $p \mid q[\mathbf{h}]$. Let $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$ be sets locally admissible at p. We say that they are ***locally good at*** p, if the corresponding restriction values modulo p depend at most on c, i.e., if

$$\begin{aligned}
&r^c_{p,i_p} = r_p(\mathcal{R}^c_{p,i_p}) && r^d_{p,i_p}[c] = r_p(\mathcal{R}^d_{p,i_p}[c]) && r^{n_2}_{p,i_p}[c] = r_p(\mathcal{R}^{n_2}_{p,i_p}[c,d])\\
&r^{n_1}_{p,i_p}[c] = r_p(\mathcal{R}^{n_1}_{p,i_p}[c,d,n_2]) && r^e_{p,i_p}[c] = r_p(\mathcal{R}^e_{p,i_p}[c,d,n_2,n_1]).
\end{aligned}$$

where r^c_{p,i_p}, $r^d_{p,i_p}[c]$, $r^{n_2}_{p,i_p}[c]$, $r^{n_1}_{p,i_p}[c]$ and $r^e_{p,i_p}[c]$ do not depend on d, n_2, n_1 or e, and if one of the following five properties holds:

(i) we have that
$$\mathcal{R}^c_{p,i_p} = \{c \in \mathcal{C} \mid c \equiv 0 \mod p\}$$
and therefore
$$r^c_{p,i_p} \geq p,$$
as well as
$$r^e_{p,i_p} \geq (cN, p^\infty);$$

(ii) we have that
$$\begin{array}{ccc} r^{n_2}_{p,i_p} r^{n_1}_{p,i_p} r^e_{p,i} \geq p^2(cN,p^\infty) & r^{n_2}_{p,i_p} r^{n_1}_{p,i_p} \geq p & r^{n_2}_{p,i_p} r^e_{p,i_p} \geq p(cN,p^\infty) \\ r^{n_2}_{p,i_p} \geq 1 & r^{n_1}_{p,i_p} r^e_{p,i_p} \geq p(cN,p^\infty) & r^{n_1}_{p,i_p} \geq 1 \\ r^e_{p,i_p} \geq (cN,p^\infty) & r^c_{p,i_p} \geq p; & \end{array}$$

(iii) we have that
$$\mathcal{R}^{n_2}_{p,i_p}[c,d] = \{n_2 \in \mathcal{N}_2 \mid n_2 \equiv 0 \mod p\}$$
and thus
$$r^{n_2}_{p,i_p} \geq p,$$
as well as
$$r^e_{p,i_p} \geq (cN, p^\infty);$$

(iv) we have that
$$\mathcal{R}^{n_1}_{p,i_p}[c,d,n_2] = \{n_1 \in \mathcal{N}_1 \mid n_1 \equiv 0 \mod p\}$$
and therefore
$$r^{n_1}_{p,i_p} \geq p,$$
as well as
$$r^e_{p,i_p} \geq (cN, p^\infty);$$

(v) we have that
$$r^{n_1}_{p,i_p} r^e_{p,i_p} \geq p(cN,p^\infty) \qquad p^{n_1}_{p,i_p} \geq (p,cN) \qquad r^e_{p,i_p} \geq \frac{p}{(p,cN)}(cN,p^\infty)$$
and
$$(c,d,n_2,n_1,e) \in \mathcal{R}^e_{p,i_p} \Rightarrow (n_1 + dn_2)^2 \equiv 4de \mod p.$$

Depending on which of the properties (i) to (v) holds, we say that p is of type R1 to R5.

Furthermore, for $i \in \mathcal{I}_{q[\mathbf{h}]}$, we call $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})_{p|q[\mathbf{h}]}$ ***good***, if for every p dividing $q[\mathbf{h}]$, $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$ is locally good at p.

For some good sets $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})_{p|q[\mathbf{h}]}$ we define
$$q[\mathbf{h};R1] = \prod_{\substack{p|q[\mathbf{h}] \\ p \text{ is of type } R1}} p \qquad q[\mathbf{h};R2] = \prod_{\substack{p|q[\mathbf{h}] \\ p \text{ is of type } R2}} p$$
$$q[\mathbf{h};R3] = \prod_{\substack{p|q[\mathbf{h}] \\ p \text{ is of type } R3}} p \qquad q[\mathbf{h};R4] = \prod_{\substack{p|q[\mathbf{h}] \\ p \text{ is of type } R4}} p$$
$$q[\mathbf{h};R5] = \prod_{\substack{p|q[\mathbf{h}] \\ p \text{ is of type } R5}} p.$$

Note that
$$q[\mathbf{h}] = q[\mathbf{h};R1]q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R4]q[\mathbf{h};R5].$$
To simplify notation, we write
$$\mathcal{R}^*_{q[\mathbf{h}],i} = \bigcap_{p\mid q[\mathbf{h}]} \mathcal{R}^*_{p,i_p}$$
where $* = c, d, n_1$ or n_2 and
$$\mathcal{R}^e_{q[\mathbf{h}],i} = \bigcap_{p\mid q[\mathbf{h}]} \mathcal{R}^e_{p,i_p} \cap \mathcal{B}_{cN}. \tag{5.17}$$

Definition 5.7.15. In the case $T(L, L)$, we define the ***threshold values***
$$t_1 = \sqrt{2}q^\varepsilon P \qquad t_3 = 4q^{2\varepsilon}Q \qquad t_4 = 4\sqrt{2}q^{2\varepsilon}QL \qquad t_5 = 144q^{4\varepsilon}Q^2L^2$$
and in the case $T(1, L^2)$, define
$$t_1 = 2q^\varepsilon PL \qquad t_3 = 4q^{2\varepsilon}QL \qquad t_4 = 4q^{2\varepsilon}QL \qquad t_5 = 64q^{4\varepsilon}Q^2L^2.$$

Lemma 5.7.16. *Let $i \in \mathcal{I}_{q[\mathbf{h}]}$ and let $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})_{p\mid q[\mathbf{h}]}$ be good sets. We have*

(i) *if $q[\mathbf{h};R1] \ge t_1$, then $\mathcal{R}^e_{q[\mathbf{h}],i} = \emptyset$;*
(ii) *if $q[\mathbf{h};R3] \ge t_3$, then $\mathcal{R}^e_{q[\mathbf{h}],i} = \emptyset$;*
(iii) *if $q[\mathbf{h};R4] \ge t_4$, then $\mathcal{R}^e_{q[\mathbf{h}],i} = \emptyset$;*
(iv) *if $q[\mathbf{h};R5] \ge t_5$, then $\mathcal{R}^e_{q[\mathbf{h}],i} = \emptyset$.*

Proof. Consider first the case $T(L, L)$.

(i) $t_1 = \sqrt{2}q^\varepsilon P$. Let $t_1 \le q[\mathbf{h};R1]$. Then
$$\mathcal{R}^c_{q[\mathbf{h}],i} \subset \bigcap_{p\mid q[\mathbf{h};R1]} \mathcal{R}^c_{p,i_p} = \{c \in \mathcal{C} \mid c \equiv 0 \mod q[\mathbf{h};R1]\} = \emptyset.$$
Hence $\mathcal{R}^e_{q[\mathbf{h}],i} \subset \mathcal{R}^c_{q[\mathbf{h}],i} \times \mathcal{D} \times \mathcal{N}_2 \times \mathcal{N}_1 \times \mathcal{E} = \emptyset$.

(ii) $t_3 = 4q^{2\varepsilon}Q$. Let $t_3 \le q[\mathbf{h};R3]$. Then, for all $(c, d) \in \mathcal{R}^d_{q[\mathbf{h}],i}$,
$$\mathcal{R}^{n_2}_{q[\mathbf{h}],i}[c, d] \subset \bigcap_{p\mid q[\mathbf{h};R3]} \mathcal{R}^{n_2}_{p,i_p}[c, d] = \{n_2 \in \mathcal{N}_2 \mid n_2 \equiv 0 \mod q[\mathbf{h};R3]\} = \emptyset.$$
Consequently $\mathcal{R}^{n_2}_{q[\mathbf{h}],i} = \emptyset$ and $\mathcal{R}^e_{q[\mathbf{h}],i} \subset \mathcal{R}^{n_2}_{q[\mathbf{h}],i} \times \mathcal{N}_1 \times \mathcal{E} = \emptyset$.

(iii) $t_4 = 4q^{2\varepsilon}QL$. Let $t_4 \le q[\mathbf{h};R4]$. Then for all $(c, d, n_2) \in \mathcal{R}^{n_2}_{q[\mathbf{h}],i}$,
$$\mathcal{R}^{n_1}_{q[\mathbf{h}],i}[c, d, n_2] \subset \bigcap_{p\mid q[\mathbf{h};R3]} \mathcal{R}^{n_1}_{p,i_p}[c, d, n_2] = \{n_1 \in \mathcal{N}_1 \mid n_1 \equiv 0 \mod q[\mathbf{h};R4]\} = \emptyset.$$
Consequently $\mathcal{R}^{n_1}_{q[\mathbf{h}],i} = \emptyset$ and $\mathcal{R}^e_{q[\mathbf{h}],i} \subset \mathcal{R}^{n_1}_{q[\mathbf{h}],i} \times \mathcal{E} = \emptyset$.

(iv) $t_5 = 144q^{4\varepsilon}Q^2L^2$. First note that
$$|n_1 + dn_2| \le |n_1| + d\,|n_2| \le 4q^{2\varepsilon}QL + 2L4q^{2\varepsilon}Q = 12q^{2\varepsilon}QL$$

and hence

$$(n_1 + dn_2)^2 \le 144q^{4\varepsilon}Q^2L^2 = t_5.$$

Furthermore

$$4de \le 16L^2 \le 144q^{4\varepsilon}Q^2L^2 = t_5.$$

Now suppose that $q[\mathbf{h}; R5] \ge t_5$. Then the condition $(n_1 + dn_2)^2 \equiv 4de \mod q[\mathbf{h}; R5]$ implies the equation

$$(n_1 + dn_2)^2 = 4de$$

in $\mathbb{Z}$. However, since $4de$ is not a square, this equation has no solution and therefore $\mathcal{R}^e_{q[\mathbf{h}],i} = \emptyset$.

Now consider the case $T(1, L^2)$.

(i) $t_1 = 2q^\varepsilon PL$. Let $t_1 \le q[\mathbf{h}; R1]$. Then

$$\mathcal{R}^c_{q[\mathbf{h}],i} \subset \bigcap_{p|q[\mathbf{h};R1]} \mathcal{R}^c_{p,i_p} = \{c \in \mathcal{C} \mid c \equiv 0 \mod q[\mathbf{h}; R1]\} = \emptyset.$$

Hence $\mathcal{R}^e_{q[\mathbf{h}],i} \subset \mathcal{R}^c_{q[\mathbf{h}],i} \times \mathcal{D} \times \mathcal{N}_2 \times \mathcal{N}_1 \times \mathcal{E} = \emptyset$.

(ii) $t_3 = 4q^{2\varepsilon}QL$. Let $t_3 \le q[\mathbf{h}; R3]$. Then, for all $(c, d) \in \mathcal{R}^d_{q[\mathbf{h}],i}$,

$$\mathcal{R}^{n_2}_{q[\mathbf{h}],i}[c, d] \subset \bigcap_{p|q[\mathbf{h};R3]} \mathcal{R}^{n_2}_{p,i_p}[c, d] = \{n_2 \in \mathcal{N}_2 \mid n_2 \equiv 0 \mod q[\mathbf{h}; R3]\} = \emptyset.$$

Consequently $\mathcal{R}^{n_2}_{q[\mathbf{h}],i} = \emptyset$ and $\mathcal{R}^e_{q[\mathbf{h}],i} \subset \mathcal{R}^{n_2}_{q[\mathbf{h}],i} \times \mathcal{N}_1 \times \mathcal{E} = \emptyset$.

(iii) $t_4 = 4q^{2\varepsilon}QL$. Let $t_4 \le q[\mathbf{h}; R4]$. Then for all $(c, d, n_2) \in \mathcal{R}^{n_2}_{q[\mathbf{h}],i}$,

$$\mathcal{R}^{n_1}_{q[\mathbf{h}],i}[c, d, n_2] \subset \bigcap_{p|q[\mathbf{h};R3]} \mathcal{R}^{n_1}_{p,i_p}[c, d, n_2] = \{n_1 \in \mathcal{N}_1 \mid n_1 \equiv 0 \mod q[\mathbf{h}; R4]\} = \emptyset.$$

Consequently $\mathcal{R}^{n_1}_{q[\mathbf{h}],i} = \emptyset$ and $\mathcal{R}^e_{q[\mathbf{h}],i} \subset \mathcal{R}^{n_1}_{q[\mathbf{h}],i} \times \mathcal{E} = \emptyset$.

(iv) $t_5 = 64q^{4\varepsilon}Q^2L^2$. First note that

$$|n_1 + dn_2| \le |n_1| + d\,|n_2| \le 4q^{2\varepsilon}QL + 4q^{2\varepsilon}QL = 8q^{2\varepsilon}QL$$

and hence

$$(n_1 + dn_2)^2 \le 64q^{4\varepsilon}Q^2L^2 = t_5.$$

Furthermore

$$4de \le 16L^2 \le 64q^{4\varepsilon}Q^2L^2 = t_5.$$

Now suppose that $q[\mathbf{h}; R5] \ge t_5$. Then the condition $(n_1 + dn_2)^2 \equiv 4de \mod q[\mathbf{h}; R5]$ implies the equation

$$(n_1 + dn_2)^2 = 4de$$

in $\mathbb{Z}$. However, since $4de$ is not a square, this equation has no solution and therefore $\mathcal{R}^e_{q[\mathbf{h}],i} = \emptyset$.

□

Theorem 5.7.17. *Let $i \in \mathcal{I}_{q[\mathbf{h}]}$. Then there exist good sets $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})_{p|q[\mathbf{h}]}$.*

We will prove this theorem in Section 5.8.

Notation. In what follows, we will denote by r_{cN} the restriction value

$$r_{cN} = r_m(\mathcal{R}^e_{q[\mathbf{h}],i})$$

where $m = \frac{cN}{(cN,q[\mathbf{h}]^\infty)}$ and $\mathcal{R}^e_{q[\mathbf{h}],i}$ is defined by equation (5.17). Hence

$$r_{cN} \geq \frac{cN}{(cN, q[\mathbf{h}]^\infty)}.$$

Furthermore, we define

$$\begin{aligned} r^e_{q[\mathbf{h}]} &= r_{q[\mathbf{h}]}\big(\mathcal{R}^e_{q[\mathbf{h}],i}[c,d,n_2,n_1]\big) & r^{n_1}_{q[\mathbf{h}]} &= r_{q[\mathbf{h}]}\big(\mathcal{R}^{n_1}_{q[\mathbf{h}],i}[c,d,n_2]\big)\\ r^{n_2}_{q[\mathbf{h}]} &= r_{q[\mathbf{h}]}\big(\mathcal{R}^{n_2}_{q[\mathbf{h}],i}[c,d]\big) & r^d_{q[\mathbf{h}]} &= r_{q[\mathbf{h}]}\big(\mathcal{R}^d_{q[\mathbf{h}],i}[c]\big)\\ r^c_{q[\mathbf{h}]} &= r_{q[\mathbf{h}]}\big(\mathcal{R}^c_{q[\mathbf{h}],i}\big). \end{aligned}$$

Note that by the properties of the restriction value, we have that

$$\begin{aligned} r^e_{q[\mathbf{h}]} &\geq \prod_{p|q[\mathbf{h}]} r^e_p[c] & r^{n_1}_{q[\mathbf{h}]} &\geq \prod_{p|q[\mathbf{h}]} r^{n_1}_p[c] & r^{n_2}_{q[\mathbf{h}]} &\geq \prod_{p|q[\mathbf{h}]} r^{n_2}_p[c]\\ r^d_{q[\mathbf{h}]} &\geq \prod_{p|q[\mathbf{h}]} r^d_p[c] & r^c_{q[\mathbf{h}]} &\geq \prod_{p|q[\mathbf{h}]} r^c_p. \end{aligned}$$

Lemma 5.7.18. *Suppose that K is (q,M)-good. Then*

$$S^{T(L,L)}[\mathbf{h}] \ll q^{6\varepsilon}P^\varepsilon Q^2 \frac{L^3}{q[\mathbf{h}]} + q^{6\varepsilon}PQ^2L^2.$$

Proof. By Lemma 5.7.11 we get that

$$S^{T(L,L)}[\mathbf{h}] \ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{C}} \sum_{d\in\mathcal{D}} \sum_{n_2\in\mathcal{N}_2} \sum_{n_1\in\mathcal{N}_1} \sum_{\substack{e\in\mathcal{E}\\ (c,d,n_2,n_1,e)\in\mathcal{B}_{cN}\\ \gamma(c,d,e,n_1,n_2)\in\mathcal{A}^i_{q[\mathbf{h}]}}} 1.$$

By Theorem 5.7.17, there exist good sets $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})_{p|q[\mathbf{h}]}$, whence

$$\begin{aligned} S^{T(L,L)}[\mathbf{h}] &\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{C}} \sum_{d\in\mathcal{D}} \sum_{n_2\in\mathcal{N}_2} \sum_{n_1\in\mathcal{N}_1} \sum_{\substack{e\in\mathcal{E}\\ (c,d,n_2,n_1,e)\in\mathcal{R}^e_{q[\mathbf{h}],i}}} 1\\ &\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{R}^c_{q[\mathbf{h}],i}} \sum_{d\in\mathcal{R}^d_{q[\mathbf{h}],i}[c]} \sum_{n_2\in\mathcal{R}^{n_2}_{q[\mathbf{h}],i}[c,d]} \sum_{n_1\in\mathcal{R}^{n_1}_{q[\mathbf{h}],i}[c,d,n_2]} \sum_{e\in\mathcal{R}^e_{q[\mathbf{h}],i}[c,d,n_2,n_1]} 1\\ &\leq \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{R}^c_{q[\mathbf{h}]}} \sum_{d\in\mathcal{R}^d_{q[\mathbf{h}]}[c]} \sum_{n_2\in\mathcal{R}^{n_2}_{q[\mathbf{h}]}[c,d]} \sum_{n_1\in\mathcal{R}^{n_1}_{q[\mathbf{h}]}[c,d,n_2]} \left(\frac{\|\mathcal{E}\|}{r^e_{q[\mathbf{h}]}r_{cN}}+1\right)\\ &\leq \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{R}^c_{q[\mathbf{h}]}} \sum_{d\in\mathcal{R}^d_{q[\mathbf{h}]}[c]} \sum_{n_2\in\mathcal{R}^{n_2}_{q[\mathbf{h}]}[c,d]} \left(\frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{E}\|}{r^e_{q[\mathbf{h}]}r_{cN}}+1\right)\\ &\leq \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{R}^c_{q[\mathbf{h}]}} \sum_{d\in\mathcal{R}^d_{q[\mathbf{h}]}[c]} \left(\frac{\|\mathcal{N}_2\|}{r^{n_2}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{E}\|}{r^e_{q[\mathbf{h}]}r_{cN}}+1\right). \end{aligned}$$

By multiplying out, we get

$$\begin{aligned}\left(\frac{\|\mathcal{N}_2\|}{r^{n_2}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{E}\|}{r^{e}_{q[\mathbf{h}]}r_{cN}}+1\right) &= \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{r^{n_2}_{q[\mathbf{h}]}r^{n_1}_{q[\mathbf{h}]}r^{e}_{q[\mathbf{h}]}r_{cN}}+\frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|}{r^{n_2}_{q[\mathbf{h}]}r^{n_1}_{q[\mathbf{h}]}}+\frac{\|\mathcal{N}_2\|\,\|\mathcal{E}\|}{r^{n_2}_{q[\mathbf{h}]}r^{e}_{q[\mathbf{h}]}r_{cN}}\\ &\quad+\frac{\|\mathcal{N}_2\|}{r^{n_2}_{q[\mathbf{h}]}}+\frac{\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{r^{n_1}_{q[\mathbf{h}]}r^{e}_{q[\mathbf{h}]}r_{cN}}+\frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}}+\frac{\|\mathcal{E}\|}{r^{e}_{q[\mathbf{h}]}r_{cN}}+1.\end{aligned}$$

Since

$$\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,,\|\mathcal{N}_2\|\,\|\mathcal{E}\|\,,\|\mathcal{N}_2\|\,,\|\mathcal{N}_1\|\,,\|\mathcal{E}\|\,,1\ll q^{4\varepsilon}Q^2L$$

we get

$$\left(\frac{\|\mathcal{N}_2\|}{r^{n_2}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{E}\|}{r^{e}_{q[\mathbf{h}]}r_{cN}}+1\right)\ll\frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{r^{n_2}_{q[\mathbf{h}]}r^{n_1}_{q[\mathbf{h}]}r^{e}_{q[\mathbf{h}]}r_{cN}}+\frac{\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{r^{n_1}_{q[\mathbf{h}]}r^{e}_{q[\mathbf{h}]}r_{cN}}+q^{4\varepsilon}Q^2L.$$

Note that because of the threshold values, either

$$\begin{aligned}q[\mathbf{h};R1]&\le t_1 & q[\mathbf{h};R3]&\le t_3\\ q[\mathbf{h};R4]&\le t_4 & q[\mathbf{h};R5]&\le t_5\end{aligned}$$

or the sum is empty. If the sum is empty, there is nothing to do, so we can assume these bounds. We therefore get

$$q[\mathbf{h};R3]\le t_3=4q^{2\varepsilon}Q\le\|\mathcal{N}_2\|$$

and hence obtain

$$\frac{\|\mathcal{N}_2\|}{q[\mathbf{h};R3]}\ge 1.$$

Let $q[\mathbf{h};R25]=q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R4]q[\mathbf{h};R5]$. Because

$$\begin{aligned}r^{n_2}_{q[\mathbf{h}]}r^{n_1}_{q[\mathbf{h}]}r^{e}_{q[\mathbf{h}]}r_{cN} &\ge r_{cN}\prod_{p|q[\mathbf{h}]}r^{n_2}_p r^{n_1}_p r^{e}_p\\ &\ge r_{cN}\left(\prod_{p|q[\mathbf{h};R1]}r^{n_2}_p r^{n_1}_p r^{e}_p\right)\left(\prod_{p|q[\mathbf{h};R2]}r^{n_2}_p r^{n_1}_p r^{e}_p\right)\left(\prod_{p|q[\mathbf{h};R3]}r^{n_2}_p r^{n_1}_p r^{e}_p\right)\\ &\quad\cdot\left(\prod_{p|q[\mathbf{h};R4]}r^{n_2}_p r^{n_1}_p r^{e}_p\right)\left(\prod_{p|q[\mathbf{h};R5]}r^{n_2}_p r^{n_1}_p r^{e}_p\right)\\ &\ge\frac{cN}{(cN,q[\mathbf{h}]^\infty)}(cN,q[\mathbf{h};R1]^\infty)q[\mathbf{h};R2]^2(cN,q[\mathbf{h};R2]^\infty)q[\mathbf{h};R3]\\ &\quad\cdot(cN,q[\mathbf{h};R3]^\infty)q[\mathbf{h};R4](cN,q[\mathbf{h};R4]^\infty)q[\mathbf{h};R5](cN,q[\mathbf{h};R5]^\infty)\\ &=q[\mathbf{h};R2]^2q[\mathbf{h};R3]q[\mathbf{h};R4]q[\mathbf{h};R5]cN\\ &\ge q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R4]q[\mathbf{h};R5]cN\\ r^{n_1}_{q[\mathbf{h}]}r^{e}_{q[\mathbf{h}]}r_{cN} &\ge q[\mathbf{h};R2]q[\mathbf{h};R4]q[\mathbf{h};R5]cN\end{aligned}$$

we get

$$\frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{r^{n_2}_{q[\mathbf{h}]}r^{n_1}_{q[\mathbf{h}]}r^{e}_{q[\mathbf{h}]}r_{cN}}\le\frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R4]q[\mathbf{h};R5]cN}=\frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{q[\mathbf{h};R25]cN}$$

$$\begin{aligned}\frac{\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{r^{n_1}_{q[\mathbf{h}]} r^{e}_{q[\mathbf{h}]} r_{cN}} &\leq \frac{\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{q[\mathbf{h};R2]q[\mathbf{h};R4]q[\mathbf{h};R5]cN} \\ &\leq \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R4]q[\mathbf{h};R5]cN} = \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{q[\mathbf{h};R25]cN}.\end{aligned}$$

Hence

$$\begin{aligned}\left(\frac{\|\mathcal{N}_2\|}{r^{n_2}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{E}\|}{r^{e}_{q[\mathbf{h}]} r_{cN}}+1\right) &\ll \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{q[\mathbf{h};R25]cN} + q^{4\varepsilon}Q^2L \\ &\ll_N \frac{q^{4\varepsilon}Q^2L^2}{q[\mathbf{h};R25]c} + q^{4\varepsilon}Q^2L\end{aligned}$$

and thus

$$\begin{aligned}S^{T(L,L)}[\mathbf{h}] &\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{R}^c_{q[\mathbf{h}]}} \sum_{d\in\mathcal{R}^d_{q[\mathbf{h}]}[c]} \left(\frac{q^{4\varepsilon}Q^2L^2}{q[\mathbf{h};R25]c} + q^{4\varepsilon}Q^2L\right) \\ &\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{R}^c_{q[\mathbf{h}]}} \left(\frac{q^{4\varepsilon}Q^2L^3}{q[\mathbf{h};R25]c} + q^{4\varepsilon}Q^2L^2\right) \\ &\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \frac{q^{4\varepsilon}Q^2L^3}{q[\mathbf{h};R25]} \sum_{\substack{1\leq c\leq\sqrt{2}q^{\varepsilon}P \\ c\equiv 0 \mod q[\mathbf{h};R1]}} \frac{1}{c} + \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} q^{5\varepsilon}PQ^2L^2 \\ &\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \frac{q^{4\varepsilon}Q^2L^3}{q[\mathbf{h};R25]} \frac{q^{\varepsilon}P^{\varepsilon}}{q[\mathbf{h};R1]} + \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} q^{5\varepsilon}PQ^2L^2 \\ &\ll q^{6\varepsilon}P^{\varepsilon}Q^2\frac{L^3}{q[\mathbf{h}]} + q^{6\varepsilon}PQ^2L^2.\end{aligned}$$

□

Lemma 5.7.19. *Suppose that K is (q,M)-good. Then*

$$S^{T(1,L^2)}[\mathbf{h}] \ll q^{9\varepsilon}P^{1+\varepsilon}Q^3\frac{L^{4+2}}{\sqrt{q[\mathbf{h}]}} + q^{4\varepsilon}PQL^2.$$

Proof. By Lemma 5.7.11 we get that

$$S^{T(1,L^2)}[\mathbf{h}] \ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{C}} \sum_{d\in\mathcal{D}} \sum_{n_2\in\mathcal{N}_2} \sum_{n_1\in\mathcal{N}_1} \sum_{\substack{e\in\mathcal{E} \\ (c,d,n_2,n_1,e)\in\mathcal{B}_{cN} \\ \gamma(c,d,e,n_1,n_2)\in\mathcal{A}^i_{q[\mathbf{h}]}}} 1.$$

By Theorem 5.7.17, there exist good sets $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})_{p|q[\mathbf{h}]}$, whence

$$\begin{aligned}S^{T(1,L^2)}[\mathbf{h}] &\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{C}} \sum_{d\in\mathcal{D}} \sum_{n_2\in\mathcal{N}_2} \sum_{n_1\in\mathcal{N}_1} \sum_{\substack{e\in\mathcal{E} \\ (c,d,n_2,n_1,e)\in\mathcal{R}^e_{q[\mathbf{h}],i}}} 1 \\ &\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{R}^c_{q[\mathbf{h}],i}} \sum_{d\in\mathcal{R}^d_{q[\mathbf{h}],i}[c]} \sum_{n_2\in\mathcal{R}^{n_2}_{q[\mathbf{h}],i}[c,d]} \sum_{n_1\in\mathcal{R}^{n_1}_{q[\mathbf{h}],i}[c,d,n_2]} \sum_{e\in\mathcal{R}^e_{q[\mathbf{h}],i}[c,d,n_2,n_1]} 1\end{aligned}$$

$$\le \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{R}^c_{q[\mathbf{h}]}} \sum_{d\in\mathcal{R}^d_{q[\mathbf{h}]}[c]} \sum_{n_2\in\mathcal{R}^{n_2}_{q[\mathbf{h}]}[c,d]} \sum_{n_1\in\mathcal{R}^{n_1}_{q[\mathbf{h}]}[c,d,n_2]} \left(\frac{\|\mathcal{E}\|}{r^e_{q[\mathbf{h}]} r_{cN}}+1\right)$$
$$\le \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{R}^c_{q[\mathbf{h}]}} \sum_{d\in\mathcal{R}^d_{q[\mathbf{h}]}[c]} \sum_{n_2\in\mathcal{R}^{n_2}_{q[\mathbf{h}]}[c,d]} \left(\frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{E}\|}{r^e_{q[\mathbf{h}]} r_{cN}}+1\right)$$
$$\le \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}} \sum_{c\in\mathcal{R}^c_{q[\mathbf{h}]}} \left(\frac{\|\mathcal{N}_2\|}{r^{n_2}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{E}\|}{r^e_{q[\mathbf{h}]} r_{cN}}+1\right).$$

By multiplying out, we get

$$\left(\frac{\|\mathcal{N}_2\|}{r^{n_2}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{E}\|}{r^e_{q[\mathbf{h}]} r_{cN}}+1\right) = \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{r^{n_2}_{q[\mathbf{h}]} r^{n_1}_{q[\mathbf{h}]} r^e_{q[\mathbf{h}]} r_{cN}} + \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|}{r^{n_2}_{q[\mathbf{h}]} r^{n_1}_{q[\mathbf{h}]}} + \frac{\|\mathcal{N}_2\|\,\|\mathcal{E}\|}{r^{n_2}_{q[\mathbf{h}]} r^e_{q[\mathbf{h}]} r_{cN}}$$
$$+ \frac{\|\mathcal{N}_2\|}{r^{n_2}_{q[\mathbf{h}]}} + \frac{\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{r^{n_1}_{q[\mathbf{h}]} r^e_{q[\mathbf{h}]} r_{cN}} + \frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}} + \frac{\|\mathcal{E}\|}{r^e_{q[\mathbf{h}]} r_{cN}} + 1.$$

Note that because of the threshold values, either

$$q[\mathbf{h}; R1] \le t_1 \qquad q[\mathbf{h}; R3] \le t_3$$
$$q[\mathbf{h}; R4] \le t_4 \qquad q[\mathbf{h}; R5] \le t_5$$

or the sum is empty. If the sum is empty, there is nothing to do, so we can assume these bounds. By defining

$$q[\mathbf{h}; R5'] = (q[\mathbf{h}; R5], cN) \qquad q[\mathbf{h}; R5''] = \frac{q[\mathbf{h}; R5]}{q[\mathbf{h}; R5']}$$

we get

$$\sqrt{q[\mathbf{h}; R5'']cN} \le \sqrt{q[\mathbf{h}; R5]cN} \le \sqrt{t_5}2q^\varepsilon PLN = 16q^{3\varepsilon}PQNL^2 = 4q^{3\varepsilon}PQN\,\|\mathcal{E}\|$$
$$\sqrt{q[\mathbf{h}; R5']q[\mathbf{h}; R4]} \le \sqrt{cNt_4} \le \sqrt{2q^\varepsilon PLNt_4} = \sqrt{8q^{3\varepsilon}PQNL^2} \le 4q^{2\varepsilon}QL\sqrt{PN}$$
$$\le \sqrt{PN}\,\|\mathcal{N}_1\|$$
$$q[\mathbf{h}; R3] \le t_3 = 4q^{2\varepsilon}QL \le \|\mathcal{N}_2\|$$

and hence obtain

$$4q^{3\varepsilon}PQN\frac{\|\mathcal{E}\|}{\sqrt{q[\mathbf{h}; R5'']cN}} \ge 1 \qquad \sqrt{PN}\frac{\|\mathcal{N}_1\|}{\sqrt{q[\mathbf{h}; R5']q[\mathbf{h}; R4]}} \ge 1$$
$$\frac{\|\mathcal{N}_2\|}{q[\mathbf{h}; R3]} \ge 1.$$

By this and because

$$r^{n_2}_{q[\mathbf{h}]} r^{n_1}_{q[\mathbf{h}]} r^e_{q[\mathbf{h}]} r_{cN} \ge q[\mathbf{h}; R2]^2 q[\mathbf{h}; R3]q[\mathbf{h}; R4]q[\mathbf{h}; R5]cN$$
$$\ge \sqrt{q[\mathbf{h}; R2]q[\mathbf{h}; R3]q[\mathbf{h}; R4]q[\mathbf{h}; R5]cN}$$
$$r^{n_2}_{q[\mathbf{h}]} r^{n_1}_{q[\mathbf{h}]} \ge q[\mathbf{h}; R2]q[\mathbf{h}; R3]q[\mathbf{h}; R4]q[\mathbf{h}; R5']$$
$$\ge \sqrt{q[\mathbf{h}; R2]q[\mathbf{h}; R3]q[\mathbf{h}; R4]q[\mathbf{h}; R5']}$$

$$
\begin{aligned}
r^{n_2}_{q[\mathbf{h}]} r^{e}_{q[\mathbf{h}]} r_{cN} &\ge q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R5'']cN \\
&\ge \sqrt{q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R5'']}cN \\
r^{n_2}_{q[\mathbf{h}]} &\ge q[\mathbf{h};R3] \ge \sqrt{q[\mathbf{h};R3]} \\
r^{n_1}_{q[\mathbf{h}]} r^{e}_{q[\mathbf{h}]} r_{cN} &\ge q[\mathbf{h};R2]q[\mathbf{h};R4]q[\mathbf{h};R5]cN \\
&\ge \sqrt{q[\mathbf{h};R2]q[\mathbf{h};R4]q[\mathbf{h};R5]}cN \\
r^{n_1}_{q[\mathbf{h}]} &\ge q[\mathbf{h};R4]q[\mathbf{h};R5'] \ge \sqrt{q[\mathbf{h};R4]q[\mathbf{h};R5']} \\
r^{e}_{q[\mathbf{h}]} r_{cN} &\ge q[\mathbf{h};R5'']cN \ge \sqrt{q[\mathbf{h};R5'']}cN
\end{aligned}
$$

we get

$$
\begin{aligned}
\frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{r^{n_2}_{q[\mathbf{h}]} r^{n_1}_{q[\mathbf{h}]} r^{e}_{q[\mathbf{h}]} r_{cN}} &\le \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R4]q[\mathbf{h};R5]}cN} = \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R25]}cN} \\
\frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|}{r^{n_2}_{q[\mathbf{h}]} r^{n_1}_{q[\mathbf{h}]}} &\le \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|}{\sqrt{q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R4]q[\mathbf{h};R5']}} \\
&\le 4q^{3\varepsilon}PQN \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R4]q[\mathbf{h};R5]}cN} \\
&= 4q^{3\varepsilon}PQN \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R25]}cN} \\
\frac{\|\mathcal{N}_2\|\,\|\mathcal{E}\|}{r^{n_2}_{q[\mathbf{h}]} r^{e}_{q[\mathbf{h}]} r_{cN}} &\le \frac{\|\mathcal{N}_2\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R5'']}cN} \\
&\le \sqrt{PN} \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R4]q[\mathbf{h};R5]}cN} = \sqrt{PN}\frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R25]}cN} \\
\frac{\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{r^{n_1}_{q[\mathbf{h}]} r^{e}_{q[\mathbf{h}]} r_{cN}} &\le \frac{\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R2]q[\mathbf{h};R4]q[\mathbf{h};R5]}cN} \\
&\le \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R2]q[\mathbf{h};R3]q[\mathbf{h};R4]q[\mathbf{h};R5]}cN} = \frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R25]}cN} \\
\frac{\|\mathcal{N}_2\|}{r^{n_2}_{q[\mathbf{h}]}} &\le \|\mathcal{N}_2\| \\
\frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}} &\le \|\mathcal{N}_1\| \\
\frac{\|\mathcal{E}\|}{r^{e}_{q[\mathbf{h}]} r_{cN}} &\le \frac{\|\mathcal{E}\|}{cN}
\end{aligned}
$$

Hence

$$
\begin{aligned}
\left(\frac{\|\mathcal{N}_2\|}{r^{n_2}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{N}_1\|}{r^{n_1}_{q[\mathbf{h}]}}+1\right)\left(\frac{\|\mathcal{E}\|}{r^{e}_{q[\mathbf{h}]} r_{cN}}+1\right) &\le (2+4q^{3\varepsilon}PQN+\sqrt{PN})\frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R25]}cN} + \|\mathcal{N}_2\| + \|\mathcal{N}_1\| + \frac{\|\mathcal{E}\|}{cN} + 1 \\
&\ll_N q^{3\varepsilon}PQ\frac{\|\mathcal{N}_2\|\,\|\mathcal{N}_1\|\,\|\mathcal{E}\|}{\sqrt{q[\mathbf{h};R25]}c} + \|\mathcal{N}_2\| + \|\mathcal{N}_1\| + \frac{\|\mathcal{E}\|}{c} + 1 \\
&\ll q^{7\varepsilon}PQ^3\frac{L^4}{\sqrt{q[\mathbf{h};R25]}c} + \frac{L^2}{c} + q^{2\varepsilon}QL
\end{aligned}
$$

and thus

$$\begin{aligned}
S^{T(1,L^2)}[\mathbf{h}] &\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}}\sum_{c\in\mathcal{R}^c_{q[\mathbf{h}]}}\left(q^{7\varepsilon}PQ^3\frac{L^4}{\sqrt{q[\mathbf{h};R25]}c}+\frac{L^2}{c}+q^{2\varepsilon}QL\right)\\
&\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}}\left(\left(q^{7\varepsilon}PQ^3\frac{L^4}{\sqrt{q[\mathbf{h};R25]}}+L^2\right)\sum_{c\in\mathcal{R}^c_{q[\mathbf{h}]}}\frac{1}{c}+q^{2\varepsilon}QL\sum_{c\in\mathcal{R}^c_{q[\mathbf{h}]}}1\right)\\
&\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}}\left(\left(q^{7\varepsilon}PQ^3\frac{L^4}{\sqrt{q[\mathbf{h};R25]}}+L^2\right)\sum_{\substack{1\leq c\leq 2q^\varepsilon PL\\ c\equiv 0 \mod q[\mathbf{h};R1]}}\frac{1}{c}+q^{3\varepsilon}QPL^2\right)\\
&\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}}\left(\left(q^{7\varepsilon}PQ^3\frac{L^4}{\sqrt{q[\mathbf{h};R25]}}+L^2\right)\frac{q^\varepsilon P^\varepsilon L^\varepsilon}{q[\mathbf{h};R1]}+q^{3\varepsilon}QPL^2\right)\\
&\ll \sum_{i\in\mathcal{I}_{q[\mathbf{h}]}}\left(q^{9\varepsilon}P^{1+\varepsilon}Q^3\frac{L^{4+\varepsilon}}{\sqrt{q[\mathbf{h}]}}+q^{3\varepsilon}QPL^2\right)\\
&\ll q^{9\varepsilon}P^{1+\varepsilon}Q^3\frac{L^{4+\varepsilon}}{\sqrt{q[\mathbf{h}]}}+q^{4\varepsilon}QPL^2.
\end{aligned}$$

□

Proposition 5.7.20. *Suppose that K is (q,M)-good. Then*

$$S[\mathbf{h}]\ll q^{9\varepsilon}P^{1+\varepsilon}Q^3\frac{L^{4+\varepsilon}}{\sqrt{q[\mathbf{h}]}}+q^{4\varepsilon}PQL^2.$$

Proof. Recall that

$$S[\mathbf{h}]=2S^{T(L,L)}[\mathbf{h}]+S^{T(1,L^2)}[\mathbf{h}].$$

By Lemma 5.7.18 and Lemma 5.7.19, we get that

$$\begin{aligned}
S[\mathbf{h}] &\ll q^{6\varepsilon}P^\varepsilon Q^2\frac{L^3}{q[\mathbf{h}]}+q^{6\varepsilon}PQ^2L^2+q^{9\varepsilon}P^{1+\varepsilon}Q^3\frac{L^{4+\varepsilon}}{\sqrt{q[\mathbf{h}]}}+q^{4\varepsilon}PQL^2\\
&\ll q^{9\varepsilon}P^{1+\varepsilon}Q^3\frac{L^{4+\varepsilon}}{\sqrt{q[\mathbf{h}]}}+q^{4\varepsilon}PQL^2.
\end{aligned}$$

□

Proof of Proposition 5.7.4. By Lemma 5.7.7,

$$M^{c\leq C,n\in\Box,\mathbf{h}}[\phi_k;d,e]\ll_N k^3q^\varepsilon\frac{PQ}{L}S[\mathbf{h}]\prod_{p|q}M^{2h_p}p^{h_p}$$

which is by Proposition 5.7.20

$$\ll k^3q^\varepsilon\frac{PQ}{L}\left(q^{9\varepsilon}P^{1+\varepsilon}Q^3\frac{L^4}{\sqrt{q[\mathbf{h}]}}+q^{4\varepsilon}PQL^2\right)\left(\prod_{p|q}M^{2h_p}p^{h_p}\right)$$

$$\ll \left(k^3 q^{10\varepsilon} P^{2+\varepsilon} Q^4 \frac{L^3}{\sqrt{q[\mathbf{h}]}} + k^3 q^{5\varepsilon} P^2 Q^2 L\right)\left(\prod_{p|q} M^{2h_p} p^{h_p}\right)$$
$$\ll k^3 q^{\frac{1}{2}+10\varepsilon} P^{2+\varepsilon} Q^4 M^{2\omega(q)} L^3 + k^3 q^{1+5\varepsilon} P^2 Q^2 M^{2\omega(q)} L$$

and analogously for $\phi_{a,b}$. □

5.8. Analysis of resonating matrices

The aim of this section is to prove Theorem 5.7.17, i.e., we will show that for $i \in \mathcal{I}_{q[\mathbf{h}]}$, there exist good sets $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})_{p|q[\mathbf{h}]}$ as defined in Definition 5.7.14. Recall that

$$\gamma(c,d,e,n_1,n_2) = \begin{pmatrix} n_1 & \frac{n_1 n_2 - e}{cN} \\ cdN & dn_2 \end{pmatrix}$$

and that

$$\gamma_p(c,d,e,n_1,n_2) \equiv \begin{pmatrix} n_1 & \frac{n_1 n_2 - e}{cN} s_p \\ cdN\overline{s_p} & dn_2 \end{pmatrix} \mod p$$

where

$$s_p \equiv \prod_{\substack{p'|q \\ p' \neq p}} \overline{p'} \mod p.$$

Lemma 5.8.1. *Let $N \in \mathbb{Z}_{\geq 1}$, p be a prime, and $(d,p) = 1$. Let $x = [x_1 : x_2], y = [y_1 : y_2] \in \mathbb{P}^1(\mathbb{F}_p)$, $x \neq y$ and let $\gamma(c,d,e,n_1,n_2) \in N^{x,y}(\mathbb{F}_p) \setminus T^{x,y}(\mathbb{F}_p)$. Then*

$$c^2 dN^2 \overline{s_p} x_1 y_1 + cn_2 dN x_2 y_1 - n_1 cN x_1 y_2 - n_1 n_2 s_p x_2 y_2 \equiv -e s_p x_2 y_2 \mod (pcN, p^\infty)$$
$$c^2 dN^2 \overline{s_p} x_1 y_1 + cn_2 dN x_1 y_2 - n_1 cN x_2 y_1 - n_1 n_2 s_p x_2 y_2 \equiv -e s_p x_2 y_2 \mod (pcN, p^\infty).$$

Proof. Let $x = [x_1 : x_2], y = [y_1 : y_2] \in \mathbb{P}^1(\mathbb{F}_p)$. Then

$$\gamma \cdot x = \gamma \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \alpha \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

for some $\alpha \in \mathbb{F}_p^\times$. This implies

$$n_1 x_1 + \frac{n_1 n_2 - e}{cN} s_p x_2 \equiv \alpha y_1 \mod p$$
$$cdN\overline{s_p} x_1 + dn_2 x_2 \equiv \alpha y_2 \mod p,$$

and hence

$$cn_1 N x_1 + n_1 n_2 x_2 - e x_2 \equiv \alpha cN y_1 \mod (pcN, p^\infty)$$
$$c^2 dN^2 x_1 + cdN n_2 x_2 \equiv \alpha cN y_2 \mod (pcN, p^\infty).$$

Since $y \in \mathbb{P}^1(\mathbb{F}_p)$, at least one of y_1 or y_2 is invertible modulo p. If y_1 is invertible modulo p, then we get

$$cn_1 N x_1 \overline{y_1} + n_1 n_2 s_p x_2 \overline{y_1} - e s_p x_2 \overline{y_1} \equiv \alpha cN \mod (pcN, p^\infty)$$

and consequently

$$c^2 dN^2 \overline{s_p} x_1 + cdN n_2 x_2 \equiv \alpha cN y_2 \equiv cn_1 N x_1 \overline{y_1} y_2 + n_1 n_2 s_p x_2 \overline{y_1} y_2 - e s_p x_2 \overline{y_1} y_2 \mod (pcN, p^\infty)$$

This can be rewritten as

$$c^2dN^2\overline{s_p}x_1y_1 + cn_2dNx_2y_1 - n_1cNx_1y_2 - n_1n_2s_px_2y_2 \equiv -es_px_2y_2 \mod (pcN, p^\infty).$$

If y_1 is not invertible modulo p, then y_2 has to be invertible modulo p. Hence

$$c^2dN^2\overline{s_p}x_1\overline{y_2} + cdNn_2x_2\overline{y_2} \equiv \alpha cN \mod (pcN, p^\infty)$$

and we get

$$cn_1Nx_1 + n_1n_2s_px_2 - es_px_2 \equiv \alpha cNy_1 \equiv c^2dN^2\overline{s_p}x_1y_1\overline{y_2} + cdNn_2x_2y_1\overline{y_2} \mod (pcN, p^\infty).$$

This can be written again as

$$c^2dN^2\overline{s_p}x_1y_1 + cn_2dNx_2y_1 - n_1cNx_1y_2 - n_1n_2s_px_2y_2 \equiv -es_px_2y_2 \mod (pcN, p^\infty).$$

Therefore, we have for every $y \in \mathbb{P}^1(\mathbb{F}_p)$ the condition

$$c^2dN^2\overline{s_p}x_1y_1 + cn_2dNx_2y_1 - n_1cNx_1y_2 - n_1n_2s_px_2y_2 \equiv -es_px_2y_2 \mod (pcN, p^\infty) \quad (5.18)$$

which completes the proof of the first equation. The second equation is obtained by interchanging x and y. ☐

Lemma 5.8.2. *Let $N \in \mathbb{Z}_{\geq 1}$, p be a prime, and $(d,p) = 1$. Let $x, y \in \mathbb{P}^1(\mathbb{F}_p)$, $x \neq y$ and let $\gamma(c,d,e,n_1,n_2) \in T^{x,y}(\mathbb{F}_p)$. Then*

$$c^2dN^2\overline{s_p}x_1^2 + cn_2dNx_1x_2 - n_1cNx_1x_2 - n_1n_2s_px_2^2 \equiv -es_px_2^2 \mod (pcN, p^\infty)$$
$$c^2dN^2\overline{s_p}y_1^2 + cn_2dNy_1y_2 - n_1cNy_1y_2 - n_1n_2s_py_2^2 \equiv -es_py_2^2 \mod (pcN, p^\infty).$$

Proof. The proof is the same as the one of Lemma 5.8.1, except that in the first equation, y is replaced by x and in the second equation, x is replaced by y. ☐

Proposition 5.8.3. *Let $N \in \mathbb{Z}_{\geq 1}$, let p be a prime with $i_p = 1$. Then there exist locally good (at p) sets $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$.*

Proof. Consider (c,d,n_2,n_1,e) such that $\gamma_p(c,d,e,n_1,n_2) \in \mathcal{A}^1_p$. Hence

$$cdN\overline{s_p} \equiv 0 \mod p.$$

Since $(dN\overline{s_p}, p) = 1$, we get that

$$c \equiv 0 \mod p.$$

Also

$$e \equiv n_1n_2 \mod cN$$

and hence by defining

$$\begin{aligned}
\mathcal{R}^c_{p,i_p} &= \{c \in \mathcal{C} \mid c \equiv 0 \mod p\} \\
\mathcal{R}^d_{p,i_p}[c] &= \mathcal{D} \\
\mathcal{R}^{n_2}_{p,i_p}[c,d] &= \mathcal{N}_2 \\
\mathcal{R}^{n_1}_{p,i_p}[c,d,n_2] &= \mathcal{N}_1 \\
\mathcal{R}^e_{p,i_p}[c,d,n_2,n_1] &= \{e \in \mathcal{E} \mid e \equiv n_1n_2 \mod (cN, p^\infty)\}
\end{aligned}$$

we can check that $(c,d,n_2,n_1,e) \in \mathcal{R}^e_{p,i_p}$, that the corresponding restriction values satisfy

$$r^c_{p,i_p} \geq p(cN, p^\infty) \qquad\qquad p^e_{p,i_p} \geq (cN, p^\infty)$$

and that $\mathcal{R}^c_{p,i_p}$ is of the desired form so that $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$ are locally good sets of type $R1$ (see Definition 5.7.14). ☐

Proposition 5.8.4. *Let $N \in \mathbb{Z}_{\geq 1}$, let p be a prime with $i_p = 2$. Then there exist locally good (at p) sets $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$.*

Proof. Consider (c, d, n_2, n_1, e) such that $\gamma_p(c, d, e, n_1, n_2) \in \mathcal{A}^2_p$. Hence

$$n_1 \equiv 0 \mod p.$$

Also

$$e \equiv n_1 n_2 \mod cN$$

and hence by defining

$$\begin{aligned}
\mathcal{R}^c_{p,i_p} &= \mathcal{C} \\
\mathcal{R}^d_{p,i_p}[c] &= \mathcal{D} \\
\mathcal{R}^{n_2}_{p,i_p}[c, d] &= \mathcal{N}_2 \\
\mathcal{R}^{n_1}_{p,i_p}[c, d, n_2] &= \{n_1 \in \mathcal{N}_1 \mid n_1 \equiv 0 \mod p\} \\
\mathcal{R}^e_{p,i_p}[c, d, n_2, n_1] &= \{e \in \mathcal{E} \mid e \equiv n_1 n_2 \mod (cN, p^\infty)\}
\end{aligned}$$

we see that $(c, d, n_2, n_1, e) \in \mathcal{R}^e_{p,i_p}$ and by checking the conditions of Definition 5.7.14 we obtain that $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$ are locally good sets of type $R4$. □

Proposition 5.8.5. *Let $N \in \mathbb{Z}_{\geq 1}$, let p be a prime with $i_p = 3$. Then there exist locally good (at p) sets $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$.*

Proof. Consider (c, d, n_2, n_1, e) such that $\gamma_p(c, d, e, n_1, n_2) \in \mathcal{A}^3_p$. Hence

$$dn_2 \equiv 0 \mod p.$$

Since $(d, p) = 1$, we get

$$n_2 \equiv 0 \mod p.$$

Also

$$e \equiv n_1 n_2 \mod cN$$

and thus by defining

$$\begin{aligned}
\mathcal{R}^c_{p,i_p} &= \mathcal{C} \\
\mathcal{R}^d_{p,i_p}[c] &= \mathcal{D} \\
\mathcal{R}^{n_2}_{p,i_p}[c, d] &= \{n_2 \in \mathcal{N}_2 \mid n_2 \equiv 0 \mod p\} \\
\mathcal{R}^{n_1}_{p,i_p}[c, d, n_2] &= \mathcal{N}_1 \\
\mathcal{R}^e_{p,i_p}[c, d, n_2, n_1] &= \{e \in \mathcal{E} \mid e \equiv n_1 n_2 \mod (cN, p^\infty)\}
\end{aligned}$$

we can check that $(c, d, n_2, n_1, e) \in \mathcal{R}^e_{p,i_p}$ and that $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$ are locally good sets of type $R3$. □

Proposition 5.8.6. *Let $N \in \mathbb{Z}_{\geq 1}$, let p be a prime with $i_p = 4$. Then there exist locally good (at p) sets $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$.*

Proof. Consider (c, d, n_2, n_1, e) such that $\gamma_p(c, d, e, n_1, n_2) \in \mathcal{A}_p^4$, i.e., γ is parabolic, so γ_p has a single fixed point in $\mathbb{P}^1(\mathbb{F}_p)$. Hence $\gamma_p \in M_2(\mathbb{F}_p)$ is a matrix with a unique eigenvalue. Therefore, the characteristic equation

$$\lambda^2 - \operatorname{tr}(\gamma_p)\lambda + \det(\gamma_p) \equiv 0 \mod p,$$

has exactly one solution. Hence, the discriminant has to be zero, i.e.,

$$\operatorname{tr}(\gamma_p)^2 - 4\det(\gamma_p) \equiv 0 \mod p.$$

This can be rewritten as

$$(n_1 + dn_2)^2 \equiv 4de \mod p.$$

We distinguish two cases: If $(p, cN) = 1$, we have $(pcN, p^\infty) = p$ and hence (since $(d, q) = 1$)

$$e \equiv \overline{4d}(n_1 + dn_2)^2 \mod (pcN, p^\infty).$$

By defining

$$\begin{aligned}
\mathcal{R}^c_{p,i_p} &= \mathcal{C} \\
\mathcal{R}^d_{p,i_p}[c] &= \mathcal{D} \\
\mathcal{R}^{n_2}_{p,i_p}[c, d] &= \mathcal{N}_2 \\
\mathcal{R}^{n_1}_{p,i_p}[c, d, n_2] &= \mathcal{N}_1 \\
\mathcal{R}^e_{p,i_p}[c, d, n_2, n_1] &= \left\{ e \in \mathcal{E} \,\middle|\, e \equiv \overline{4d}(n_1 + dn_2)^2 \mod (pcN, p^\infty) \right\}
\end{aligned}$$

we can check that $(c, d, n_2, n_1, e) \in \mathcal{R}^e_{p,i_p}$ and that the corresponding restriction values satisfy

$$r^{n_1}_{p,i_p} r^e_{p,i_p} \geq p(cN, p^\infty) \qquad p^{n_1}_{p,i_p} \geq 1 = (p, cN) \qquad r^e_{p,i_p} \geq p = \frac{p}{(p, cN)}(cN, p^\infty)$$

and that for all $(c, d, n_2, n_1, e) \in \mathcal{R}^e_{p,i_p}$

$$(n_1 + dn_2)^2 \equiv 4de \mod p.$$

Thus we have verified that in this case $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$ are locally good sets of type R5.

If $(p, cN) \neq 1$, we have

$$(n_1 + dn_2)^2 \equiv 4dn_1n_2 \mod p$$

since

$$e \equiv n_1n_2 \mod cN$$

and hence

$$n_1^2 + 2dn_1n_2 + d^2n_2^2 \equiv 4dn_1n_2 \mod p.$$

But this means

$$(n_1 - dn_2)^2 \equiv n_1^2 - 2dn_1n_2 + d^2n_2^2 \equiv 0 \mod p.$$

Therefore

$$n_1 \equiv dn_2 \mod p.$$

Together with

$$e \equiv n_1n_2 \mod (cN, p^\infty)$$

and by defining

$$\begin{aligned}\mathcal{R}^{c}_{p,i_p} &= \mathcal{C}\\ \mathcal{R}^{d}_{p,i_p}[c] &= \mathcal{D}\\ \mathcal{R}^{n_2}_{p,i_p}[c,d] &= \mathcal{N}_2\\ \mathcal{R}^{n_1}_{p,i_p}[c,d,n_2] &= \{n_1 \in \mathcal{N}_1 \mid n_1 \equiv dn_2 \mod p\}\\ \mathcal{R}^{e}_{p,i_p}[c,d,n_2,n_1] &= \{e \in \mathcal{E} \mid e \equiv n_1n_2 \mod (cN, p^\infty)\}\end{aligned}$$

we can check that $(c,d,n_2,n_1,e) \in \mathcal{R}^{e}_{p,i_p}$ and that the corresponding restriction values satisfy

$$r^{n_1}_{p,i_p} r^{e}_{p,i_p} \geq p(cN, p^\infty) \qquad p^{n_1}_{p,i_p} \geq p = (p, cN) \qquad r^{e}_{p,i_p} \geq (cN, p^\infty) = \frac{p}{(p, cN)}(cN, p^\infty)$$

and that for all $(c,d,n_2,n_1,e) \in \mathcal{R}^{e}_{p,i_p}$

$$(n_1 + dn_2)^2 \equiv 4de \mod p.$$

Thus we see that also in this case $(\mathcal{R}^{c}_{p,i_p}, \mathcal{R}^{d}_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^{e}_{p,i_p})$ are locally good sets of type R5. □

Proposition 5.8.7. *Let $N \in \mathbb{Z}_{\geq 1}$, let p be a prime, let $x, y \in \mathbb{P}^1(\mathbb{F}_p)$, $x \neq y$ and let $i_p = (5, x, y)$. Then there exist locally good (at p) sets $(\mathcal{R}^{c}_{p,i_p}, \mathcal{R}^{d}_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^{e}_{p,i_p})$.*

Proof. Consider (c,d,n_2,n_1,e) such that $\gamma_p(c,d,e,n_1,n_2) \in \mathcal{A}_p^{(5,x,y)}$. By Lemma 5.8.2, we have that

$$\begin{aligned}c^2dN^2\overline{s_p}x_1^2 + cn_2dNx_1x_2 - n_1cNx_1x_2 - n_1n_2s_px_2^2 &\equiv -es_px_2^2 \mod (pcN, p^\infty)\\ c^2dN^2\overline{s_p}y_1^2 + cn_2dNy_1y_2 - n_1cNy_1y_2 - n_1n_2s_py_2^2 &\equiv -es_py_2^2 \mod (pcN, p^\infty).\end{aligned}$$

We consider now different cases.

(i) If $p \mid x_2$ and $p \nmid y_2$, then

$$c^2dN^2\overline{s_p}x_1^2 + (e - n_1n_2)s_px_2^2 \equiv 0 \mod (pcN, p^\infty)$$

and since $cN \mid (e - n_1n_2)$ we get (independent of whether $p|cN$ or not)

$$cdN\overline{s_p}x_1^2 \equiv 0 \mod p.$$

Hence

$$c \equiv 0 \mod p.$$

Furthermore

$$e \equiv n_1n_2 + n_1cN\overline{s_p}y_1\overline{y_2} - cn_2dN\overline{s_p}y_1\overline{y_2} - c^2dN^2\overline{s_p}^2y_1^2\overline{y_2}^2 \mod (pcN, p^\infty).$$

By defining

$$\begin{aligned}\mathcal{R}^{c}_{p,i_p} &= \{c \in \mathcal{C} \mid c \equiv 0 \mod p\}\\ \mathcal{R}^{d}_{p,i_p}[c] &= \mathcal{D}\\ \mathcal{R}^{n_2}_{p,i_p}[c,d] &= \mathcal{N}_2\end{aligned}$$

$$\begin{aligned}\mathcal{R}^{n_1}_{p,i_p}[c,d,n_2] &= \mathcal{N}_1\\ \mathcal{R}^{e}_{p,i_p}[c,d,n_2,n_1] &= \big\{e\in\mathcal{E}\;\big|\; e\equiv n_1n_2+n_1cN\overline{s_p}y_1\overline{y_2}-cn_2dN\overline{s_p}y_1\overline{y_2}-c^2dN^2\overline{s_p}^2y_1^2 \mod (pcN,p^\infty)\big\}\end{aligned}$$

we can check that $(c,d,n_2,n_1,e)\in\mathcal{R}^e_{p,i_p}$ and that the corresponding restriction values satisfy

$$r^c_{p,i_p}\geq p \qquad\qquad p^e_{p,i_p}\geq (cN,p^\infty)$$

hence $(\mathcal{R}^c_{p,i_p},\mathcal{R}^d_{p,i_p},\mathcal{R}^{n_2}_{p,i_p},\mathcal{R}^{n_1}_{p,i_p},\mathcal{R}^e_{p,i_p})$ are locally good sets of type R1.

(ii) If $p\mid y_2$ and $p\nmid x_2$, then we get analogously to case (i) locally good sets of type R1.

(iii) If $p\nmid x_2$ and $p\nmid y_2$, we have

$$\begin{aligned}e&\equiv n_1n_2+cN\overline{s_p}x_1\overline{x_2}(n_1-n_2d-cdN\overline{s_p}x_1\overline{x_2}) \mod (pcN,p^\infty)\\ e&\equiv n_1n_2+cN\overline{s_p}y_1\overline{y_2}(n_1-n_2d-cdN\overline{s_p}y_1\overline{y_2}) \mod (pcN,p^\infty).\end{aligned}$$

Hence

$$(x_1\overline{x_2}-y_1\overline{y_2})n_1\equiv\big(dn_2+cdN\overline{s_p}(x_1\overline{x_2}+y_1\overline{y_2})\big)(x_1\overline{x_2}-y_1\overline{y_2}) \mod p$$

and thus

$$n_1\equiv dn_2+cdN\overline{s_p}(x_1\overline{x_2}+y_1\overline{y_2}) \mod p.$$

By defining

$$\begin{aligned}\mathcal{R}^c_{p,i_p}&=\mathcal{C}\\ \mathcal{R}^d_{p,i_p}[c]&=\mathcal{D}\\ \mathcal{R}^{n_2}_{p,i_p}[c,d]&=\mathcal{N}_2\\ \mathcal{R}^{n_1}_{p,i_p}[c,d,n_2]&=\{n_1\in\mathcal{N}_1\mid n_1\equiv dn_2+cdN\overline{s_p}(x_1\overline{x_2}+y_1\overline{y_2}) \mod p\}\\ \mathcal{R}^{e}_{p,i_p}[c,d,n_2,n_1]&=\{e\in\mathcal{E}\mid e\equiv n_1n_2+cNs_px_1\overline{x_2}(n_1-n_2d-cdN\overline{s_p}x_1\overline{x_2}) \mod (pcN,p^\infty)\}\end{aligned}$$

we again can check all inequalities to see that $(\mathcal{R}^c_{p,i_p},\mathcal{R}^d_{p,i_p},\mathcal{R}^{n_2}_{p,i_p},\mathcal{R}^{n_1}_{p,i_p},\mathcal{R}^e_{p,i_p})$ are locally good sets of type R2 with $(c,d,n_2,n_1,e)\in\mathcal{R}^e_{p,i_p}$.

□

Proposition 5.8.8. *Let $N\in\mathbb{Z}_{\geq1}$, let p be a prime, let $x,y\in\mathbb{P}^1(\mathbb{F}_p)$, $x\neq y$ and let $i_p=(6,x,y)$. Then there exist locally good (at p) sets $(\mathcal{R}^c_{p,i_p},\mathcal{R}^d_{p,i_p},\mathcal{R}^{n_2}_{p,i_p},\mathcal{R}^{n_1}_{p,i_p},\mathcal{R}^e_{p,i_p})$.*

Proof. Consider (c,d,n_2,n_1,e) such that $\gamma_p(c,d,e,n_1,n_2)\in\mathcal{A}_p^{(6,x,y)}$. By Lemma 5.8.1, we have that

$$c^2dN^2\overline{s_p}x_1y_1+cn_2dNx_2y_1-n_1cNx_1y_2-n_1n_2s_px_2y_2\equiv -es_px_2y_2 \mod (pcN,p^\infty) \quad (5.19)$$
$$c^2dN^2\overline{s_p}x_1y_1+cn_2dNx_1y_2-n_1cNx_2y_1-n_1n_2s_px_2y_2\equiv -es_px_2y_2 \mod (pcN,p^\infty). \quad (5.20)$$

We consider now different cases.

(i) Let $p\mid x_1$ and $p\mid y_2$. Then (5.19) becomes

$$n_2\equiv 0 \mod p$$

and (5.20) becomes

$$n_1\equiv 0 \mod p.$$

By defining

$$\begin{aligned}
\mathcal{R}^{c}_{p,i_p} &= \mathcal{C}\\
\mathcal{R}^{d}_{p,i_p}[c] &= \mathcal{D}\\
\mathcal{R}^{n_2}_{p,i_p}[c,d] &= \{n_2 \in \mathcal{N}_2 \mid n_2 \equiv 0 \mod p\}\\
\mathcal{R}^{n_1}_{p,i_p}[c,d,n_2] &= \{n_1 \in \mathcal{N}_1 \mid n_1 \equiv 0 \mod p\}\\
\mathcal{R}^{e}_{p,i_p}[c,d,n_2,n_1] &= \{e \in \mathcal{E} \mid e \equiv n_1 n_2 \mod (cN, p^\infty)\}
\end{aligned}$$

we can check that $(\mathcal{R}^{c}_{p,i_p}, \mathcal{R}^{d}_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^{e}_{p,i_p})$ are locally good sets of type R2 with $(c,d,n_2,n_1,e) \in \mathcal{R}^{e}_{p,i_p}$.

(ii) Let $p \mid x_2$ and $p \mid y_1$. Then (5.19) becomes

$$n_1 \equiv 0 \mod p$$

and (5.20) becomes

$$n_2 \equiv 0 \mod p.$$

Hence we can define the same sets as in case (i) and analogously conclude that $(\mathcal{R}^{c}_{p,i_p}, \mathcal{R}^{d}_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^{e}_{p,i_p})$ are locally good sets of type R2 with $(c,d,n_2,n_1,e) \in \mathcal{R}^{e}_{p,i_p}$.

(iii) Let $p \mid x_1$ and $p \nmid y_1 y_2$. Then (5.19) becomes

$$cn_2 dNx_2 y_1 - n_1 n_2 s_p x_2 y_2 \equiv -e s_p x_2 y_2 \mod (pcN, p^\infty)$$

and (5.20) becomes

$$-n_1 cNx_2 y_1 - n_1 n_2 s_p x_2 y_2 \equiv -e s_p x_2 y_2 \mod (pcN, p^\infty).$$

Hence

$$\begin{aligned}
e &\equiv n_1 n_2 + n_1 cN\overline{s_p} y_1 \overline{y_2} \mod (pcN, p^\infty),\\
n_1 &\equiv -dn_2 \mod p.
\end{aligned}$$

By defining

$$\begin{aligned}
\mathcal{R}^{c}_{p,i_p} &= \mathcal{C}\\
\mathcal{R}^{d}_{p,i_p}[c] &= \mathcal{D}\\
\mathcal{R}^{n_2}_{p,i_p}[c,d] &= \mathcal{N}_2\\
\mathcal{R}^{n_1}_{p,i_p}[c,d,n_2] &= \{n_1 \in \mathcal{N}_1 \mid n_1 \equiv -dn_2 \mod p\}\\
\mathcal{R}^{e}_{p,i_p}[c,d,n_2,n_1] &= \{e \in \mathcal{E} \mid e \equiv n_1 n_2 + n_1 cN\overline{s_p} y_1 \overline{y_2} \mod (pcN, p^\infty)\}
\end{aligned}$$

we can check that $(\mathcal{R}^{c}_{p,i_p}, \mathcal{R}^{d}_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^{e}_{p,i_p})$ are locally good sets of type R2 with $(c,d,n_2,n_1,e) \in \mathcal{R}^{e}_{p,i_p}$.

(iv) Let $p \mid x_2$ and $p \nmid y_1 y_2$. Then (5.19) becomes

$$cdN\overline{s_p} x_1 y_1 - n_1 x_1 y_2 \equiv 0 \mod p$$

and (5.20) becomes

$$cdN\overline{s_p} x_1 y_1 + n_2 d x_1 y_2 \equiv 0 \mod p.$$

Hence

$$\begin{aligned} e &\equiv n_1 n_2 \mod (cN, p^\infty) \\ n_1 &\equiv cdN\overline{s_p}y_1\overline{y_2} \mod p \\ n_2 &\equiv -cN\overline{s_p}y_1\overline{y_2} \mod p. \end{aligned}$$

By defining

$$\begin{aligned} \mathcal{R}^c_{p,i_p} &= \mathcal{C} \\ \mathcal{R}^d_{p,i_p}[c] &= \mathcal{D} \\ \mathcal{R}^{n_2}_{p,i_p}[c,d] &= \{n_2 \in \mathcal{N}_2 \mid n_2 \equiv -cN\overline{s_p}y_1\overline{y_2} \mod p\} \\ \mathcal{R}^{n_1}_{p,i_p}[c,d,n_2] &= \{n_1 \in \mathcal{N}_1 \mid n_1 \equiv cdN\overline{s_p}y_1\overline{y_2} \mod p\} \\ \mathcal{R}^e_{p,i_p}[c,d,n_2,n_1] &= \{e \in \mathcal{E} \mid e \equiv n_1 n_2 \mod (cN, p^\infty)\} \end{aligned}$$

we can check that $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$ are locally good sets of type R2 with $(c,d,n_2,n_1,e) \in \mathcal{R}^e_{p,i_p}$.

(v) Let $p \nmid x_1x_2$ and $p \nmid y_1y_2$. Then (5.19) becomes

$$e \equiv n_1n_2 + n_1cN\overline{s_p}x_1\overline{x_2} - c^2dN^2\overline{s_p}^2x_1\overline{x_2}y_1\overline{y_2} - cn_2dN\overline{s_p}y_1\overline{y_2} \mod (pcN, p^\infty)$$

and (5.20) becomes

$$e \equiv n_1n_2 + n_1cN\overline{s_p}y_1\overline{y_2} - c^2dN^2\overline{s_p}^2x_1\overline{x_2}y_1\overline{y_2} - cn_2dN\overline{s_p}x_1\overline{x_2} \mod (pcN, p^\infty).$$

Hence

$$\begin{aligned} e &\equiv n_1n_2 + n_1cN\overline{s_p}x_1\overline{x_2} - c^2dN^2\overline{s_p}^2x_1\overline{x_2}y_1\overline{y_2} - cn_2dN\overline{s_p}y_1\overline{y_2} \mod (pcN, p^\infty) \\ n_1 &\equiv -dn_2 \mod p. \end{aligned}$$

By defining

$$\begin{aligned} \mathcal{R}^c_{p,i_p} &= \mathcal{C} \\ \mathcal{R}^d_{p,i_p}[c] &= \mathcal{D} \\ \mathcal{R}^{n_2}_{p,i_p}[c,d] &= \mathcal{N}_2 \\ \mathcal{R}^{n_1}_{p,i_p}[c,d,n_2] &= \{n_1 \in \mathcal{N}_1 \mid n_1 \equiv -dn_2 \mod p\} \\ \mathcal{R}^e_{p,i_p}[c,d,n_2,n_1] &= \left\{e \in \mathcal{E} \;\middle|\; e \equiv n_1n_2 + n_1cN\overline{s_p}x_1\overline{x_2} - c^2dN^2\overline{s_p}^2x_1\overline{x_2}y_1\overline{y_2} - cn_2dN\overline{s_p}y_1\overline{y_2} \mod (pcN, p^\infty)\right\} \end{aligned}$$

we can check that $(\mathcal{R}^c_{p,i_p}, \mathcal{R}^d_{p,i_p}, \mathcal{R}^{n_2}_{p,i_p}, \mathcal{R}^{n_1}_{p,i_p}, \mathcal{R}^e_{p,i_p})$ are locally good sets of type R2 with $(c,d,n_2,n_1,e) \in \mathcal{R}^e_{p,i_p}$.

This completes the proof. □

Proof of Theorem 5.7.17. This is a direct consequence of Propositions 5.8.3, 5.8.4, 5.8.5, 5.8.6, 5.8.7 and 5.8.8. □

6. Sums over Primes to Squarefree Moduli

In this section we sketch the proof of Theorem 2.6.3. To prove Theorem 2.6.3, it is enough to follow the proof of Theorem 1.5 in [23] and make some minor adaptions, which includes replacing results of [22] by results derived in this thesis. We will now give a quick outline of the proof of [23, Theorem 1.5] and indicate what modifications need to be made to obtain the slightly more general Theorem 2.6.3.

As explained on page 1693 in [23], one uses Heath-Brown's identity as well as a smooth partition of unity (see [23, Lemma 4.3]) to decompose

$$\sum_n \Lambda(n)K(n)V\Big(\frac{n}{Pq}\Big)$$

into a linear combination, with coefficients bounded by $O_k(\log q)$, of $O(\log^{2k} q)$ sums of the shape

$$\sum_{m_1,\dots,m_k} \alpha_1(m_1)\cdots\alpha_k(m_k) \sum_{n_1,\dots,n_k} V_1(n_1)\cdots V_k(n_k)V\Big(\frac{m_1\cdots m_k n_1\cdots n_k}{Pq}\Big)K(m_1\cdots m_k n_1\cdots n_k)$$

for some integral parameter $k \geq 2$, where

(i) $\mathbf{M} = (M_1,\dots,M_k)$, $\mathbf{N} = (N_1,\dots,N_k)$ are k-tuples of parameters in $[\frac{1}{2}, 2Pq]^{2k}$ which satisfy
$$N_1 \geq N_2 \geq \cdots N_k, \quad M_i \leq (Pq)^{\frac{1}{k}}, \quad M_1\cdots M_k N_1\cdots N_k \asymp_k Pq;$$

(ii) the arithmetic functions $m \longmapsto \alpha_i(m)$ are bounded and supported in $[M_i/2, 2M_i]$;

(iii) the smooth functions $V_i(x)$ are compactly supported in $[N_i/2, 2N_i]$, and their derivatives satisfy
$$y^\ell V_i^{(\ell)}(y) \ll 1$$
for all $y \geq 1$, where the implicit constant depends only on ℓ.

Compare this to equation (4.1) in [23]. The n_i's are called the smooth variables and the m_i's are called the nonsmooth variables. Normally, the only thing which one can exploit about the functions α_i is, that they are supported on short intervals. The smooth functions V_i on the other hand may be supported on long intervals. The sums are categorized according to the number of long smooth variables. If there is one very long smooth variable, the sum is of type I, if there are two relatively long smooth variables, the sum is of type I_2, if there are three relatively long smooth variables, the sum is of type I_3 and so on (see p. 1693 and 1694 in [23]). The estimate of such sums I_r becomes harder, as r increases. Hence one treats this sums for small r's and the remaining sums are then called sums of type II.

For the proof of Theorem 2.6.3 it is enough to deal with sums of type I_2 and to consider all other sums as of type II. In [23], the estimate of sums of type I_2 is done in Theorem 1.16, while the estimate of the sums of type II is equation (1.6) in Theorem 1.17. Combining this two results leads to [23, Theorem 1.5], the proof is carried out in [23, Chapter 4]. To prove Theorem 2.6.3, we have to adapt the proof of Theorem 1.5 in [23] to K modulo q squarefree as in the assumptions of Theorem 2.6.3. Since the part of the proof which is covered in Chapter 4 of [23] is purely analytic and does not rely on whether q is prime or squarefree, this part of the proof goes through without any modification. However, the proofs of Theorem 1.16 and Theorem 1.17 in [23] need to be modified slightly to get analogous statements for a more general function K. How one has to do this is explained in the next two sections.

6.1. Estimate of type I_2 sums

To deal with type I_2 sums for q squarefree, we need a slightly more general version of Theorem 1.16 in [23], which is Theorem 3.3.2, which we proved already.

6.2. Estimate of type II sums

The estimate for type II sums which we need is a general version of equation (1.6) of Theorem 1.17 in [23], which reads as follows.

Theorem 6.2.1. *Let q be a squarefree number and let $K\colon \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$ be a q-primeperiodic function. Assume that K is (q, D)-non-exceptional. Let $M, N \geq 1$ be parameters, and let $(\alpha_m)_m$, $(\beta_n)_n$ be sequences supported on $[M/2, 2M]$ and $[N/2, 2N]$, respectively. Then we have that*

$$\sum_{\substack{m,n\\(m,q)=1}} \alpha_m \beta_n K(mn) \ll \|\alpha\| \, \|\beta\| \, (MN)^{\frac{1}{2}} \Big(\frac{1}{q^{\frac{1}{4}}} + \frac{1}{M^{\frac{1}{2}}} + \frac{q^{\frac{1}{4}} \log^{\frac{1}{2}} q}{N^{\frac{1}{2}}} \Big),$$

where

$$\|\alpha\|^2 = \sum_m |\alpha_m|^2, \qquad \|\beta\|^2 = \sum_n |\beta_n|^2.$$

The proof of the original result is given in Chapter 3 of [23]. To prove Theorem 6.2.1, we start analogously. We consider the bilinear form

$$T = \sum_{\substack{m\\(m,q)=1}} \sum_n \alpha_m \beta_n K(mn)$$

which, by taking the support of (α_m) and (β_n) into account, can be rewritten as

$$= \sum_{\frac{N}{2} \leq n \leq 2N} \beta_n \sum_{\substack{\frac{M}{2} \leq m \leq 2M\\(m,q)=1}} \alpha_m K(mn).$$

Therefore, by the Cauchy-Schwarz inequality, we obtain

$$\begin{aligned} |T|^2 &\leq \|\beta\|^2 \sum_{\frac{N}{2} \leq n \leq 2N} \Bigg| \sum_{\substack{\frac{M}{2} \leq m \leq 2M\\(m,q)=1}} \alpha_m K(mn) \Bigg|^2 \\ &= \|\beta\|^2 \sum_{\substack{\frac{M}{2} \leq m_1, m_2 \leq 2M\\(m_1 m_2, q)=1}} \overline{\alpha_{m_1}} \alpha_{m_2} \sum_{\frac{N}{2} \leq n \leq 2N} \overline{K(m_1 n)} K(m_2 n). \end{aligned} \tag{6.1}$$

By the completion method (see (3.2) in [23]), we get that

$$\sum_{\frac{N}{2} \leq n \leq 2N} \overline{K(m_1 n)} K(m_2 n) = \frac{1}{q} \sum_{\frac{N}{2} \leq n \leq 2N} \sum_{m \in \mathbb{Z}/q\mathbb{Z}} \overline{K(m_1 m)} K(m_2 m) \sum_{h \in \mathbb{Z}/q\mathbb{Z}} e\Big(\frac{(n-m)h}{q} \Big)$$

$$
\begin{aligned}
&= \sum_{h\in\mathbb{Z}/q\mathbb{Z}} \frac{1}{q} \sum_{\frac{N}{2}\le n\le 2N} e\Big(\frac{nh}{q}\Big) \sum_{m\in\mathbb{Z}/q\mathbb{Z}} \overline{K(m_1m)}K(m_2m)e\Big(\frac{-mh}{q}\Big)\\
&= \frac{1}{q} \sum_{\frac{N}{2}\le n\le 2N} \sum_{m\in\mathbb{Z}/q\mathbb{Z}} \overline{K(m_1m)}K(m_2m)\\
&\quad + \sum_{h\in\mathbb{Z}/q\mathbb{Z}\setminus\{0\}} \frac{1}{q} \sum_{\frac{N}{2}\le n\le 2N} e\Big(\frac{-nh}{q}\Big) \sum_{m\in\mathbb{Z}/q\mathbb{Z}} \overline{K(m_1m)}K(m_2m)e\Big(\frac{hm}{q}\Big)\\
&= \frac{N}{q}\,|\mathcal{C}(m_1,m_2,0,K)| + \sum_{0<|h|\le\frac{q}{2}} \frac{1}{q}\,|\mathcal{C}(m_1,m_2,h,K)| \left|\sum_{\frac{N}{2}\le n\le 2N} e\Big(\frac{-nh}{q}\Big)\right|.
\end{aligned}
$$

Clearly

$$\frac{1}{q}\sum_{\frac{N}{2}\le n\le 2N} e\Big(\frac{-nh}{q}\Big) \ll \frac{N}{q}.$$

But we have also

$$\frac{1}{q}\sum_{\frac{N}{2}\le n\le 2N} e\Big(\frac{-nh}{q}\Big) \ll \frac{1}{q}\frac{1-e\Big(\frac{2hN}{q}\Big)}{1-e\Big(\frac{h}{q}\Big)} \ll \frac{1}{q}\frac{1}{1-e\Big(\frac{h}{q}\Big)} \ll \frac{1}{q}\frac{q}{h} = \frac{1}{h}$$

since for $1\le h\le \frac{q}{2}$

$$\left|1-e\Big(\frac{h}{q}\Big)\right| = \left|e\Big(\frac{-h}{2q}\Big) - e\Big(\frac{h}{2q}\Big)\right| = \left|\sin\Big(\frac{\pi h}{q}\Big)\right| \gg \frac{h}{q}.$$

Therefore

$$\sum_{\frac{N}{2}\le n\le 2N} \overline{K(m_1n)}K(m_2n) \ll \frac{N}{q}\left|\mathcal{C}'\big(K;(m_1\overline{m_2},0)\big)\right| + \sum_{0<|h|\le\frac{q}{2}} \min\Big(\frac{1}{|h|},\frac{N}{q}\Big)\left|\mathcal{C}'\big(K;(m_1\overline{m_2},h\overline{m_2})\big)\right|.$$

Combining this with (6.1) gives

$$
\begin{aligned}
|T|^2 &\ll \|\beta\|^2 \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M\\ (m_1m_2,q)=1}} \overline{\alpha_{m_1}}\alpha_{m_2}\frac{N}{q}\left|\mathcal{C}'\big(K;(m_1\overline{m_2},0)\big)\right|\\
&\quad + \|\beta\|^2 \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M\\ (m_1m_2,q)=1}} \overline{\alpha_{m_1}}\alpha_{m_2} \sum_{0<|h|\le\frac{q}{2}} \min\Big(\frac{1}{|h|},\frac{N}{q}\Big)\left|\mathcal{C}'\big(K;(m_1\overline{m_2},h\overline{m_2})\big)\right|\\
&= \|\beta\|^2 \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M\\ (m_1m_2,q)=1}} \overline{\alpha_{m_1}}\alpha_{m_2}\frac{N}{q}\prod_{p|q}\left|\mathcal{C}'\big(K_p;(m_1\overline{m_2},0)\big)\right|\\
&\quad + \|\beta\|^2 \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M\\ (m_1m_2,q)=1}} \overline{\alpha_{m_1}}\alpha_{m_2} \sum_{0<|h|\le\frac{q}{2}} \min\Big(\frac{1}{|h|},\frac{N}{q}\Big)\prod_{p|q}\left|\mathcal{C}'\big(K_p;(m_1\overline{m_2},s_ph\overline{m_2})\big)\right|
\end{aligned}
$$

Now, in contrast to the case where q is a prime, to estimate the $\mathcal{C}'\big(K;(m,h)\big)$'s, we also need to consider mixed cases, where for some $p|q$, we can apply the bound $\ll p^{\frac{1}{2}}$, while for another $p|q$ we may only by able to apply the trivial bound. To implement this idea, we make a definition analogous to Definition 5.7.2.

Definition 6.2.2. Fix a squarefree number q. Then we associate to every $(m,h) \in (\mathbb{Z}/q\mathbb{Z})^\times \times \mathbb{Z}/q\mathbb{Z}$ its type $\mathbf{T}[(m,h)]$ which is a vector $\mathbf{T}[(m,h)] = \big(T[(m,h)]_p\big)_{p|q}$ given by

$$T[(m,h)]_p = \begin{cases} \frac{1}{2} & \text{if } (m,h) \notin \mathbf{H}_{K_p,M}, \\ 1 & \text{if } (m,h) \in \mathbf{H}_{K_p,M}. \end{cases}$$

We denote the space of all possible types by $\mathbf{H} = \left\{\frac{1}{2}, 1\right\}^{\omega(q)}$.

We then write

$$\begin{aligned}
&\|\beta\|^2 \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M \\ (m_1m_2,q)=1}} \overline{\alpha_{m_1}}\alpha_{m_2} \frac{N}{q} \prod_{p|q} \big|\mathcal{C}'\big(K_p;(m_1\overline{m_2},0)\big)\big| \\
&= \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M \\ (m_1m_2,q)=1 \\ T[(m_1\overline{m_2},0)]=\mathbf{h}}} \overline{\alpha_{m_1}}\alpha_{m_2} \frac{N}{q} \prod_{p|q} \big|\mathcal{C}'\big(K_p;(m_1\overline{m_2},0)\big)\big| \\
&\ll \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M \\ (m_1m_2,q)=1 \\ T[(m_1\overline{m_2},0)]=\mathbf{h}}} |\alpha_{m_1}|\,|\alpha_{m_2}| \frac{N}{q} \prod_{p|q} p^{h_p} \\
&\ll \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \left(\frac{N}{q}\prod_{p|q} p^{h_p}\right) \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M \\ (m_1m_2,q)=1 \\ T[(m_1\overline{m_2},0)]=\mathbf{h}}} \big(\,|\alpha_{m_1}|^2 + |\alpha_{m_2}|^2\,\big) \\
&= \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \left(\frac{N}{q}\prod_{p|q} p^{h_p}\right)\left(\sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M \\ (m_1m_2,q)=1 \\ T[(m_1\overline{m_2},0)]=\mathbf{h}}} |\alpha_{m_1}|^2 + \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M \\ (m_1m_2,q)=1 \\ T[(m_1\overline{m_2},0)]=\mathbf{h}}} |\alpha_{m_2}|^2 \right) \\
&= \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \left(\frac{N}{q}\prod_{p|q} p^{h_p}\right)\Bigg(\sum_{\substack{\frac{M}{2}\le m_1\le 2M \\ (m_1,q)=1}} |\alpha_{m_1}|^2 \sum_{\substack{\frac{M}{2}\le m_2\le 2M \\ (m_2,q)=1 \\ T[(m_1\overline{m_2},0)]=\mathbf{h}}} 1 \\
&\qquad + \sum_{\substack{\frac{M}{2}\le m_2\le 2M \\ (m_2,q)=1}} |\alpha_{m_2}|^2 \sum_{\substack{\frac{M}{2}\le m_1\le 2M \\ (m_1,q)=1 \\ T[(m_1\overline{m_2},0)]=\mathbf{h}}} 1 \Bigg) \\
&= \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \left(\frac{N}{q}\prod_{p|q} p^{h_p}\right)\Bigg(\sum_{\substack{\frac{M}{2}\le m_1\le 2M \\ (m_1,q)=1}} |\alpha_{m_1}|^2 \left(\frac{M}{q[\mathbf{h}]}+1\right) \\
&\qquad + \sum_{\substack{\frac{M}{2}\le m_2\le 2M \\ (m_2,q)=1}} |\alpha_{m_2}|^2 \left(\frac{M}{q[\mathbf{h}]}+1\right)\Bigg) \\
&\ll \|\alpha\|^2\,\|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \left(\frac{N}{q}\prod_{p|q} p^{h_p}\right)\left(\frac{M}{q[\mathbf{h}]}+1\right)
\end{aligned}$$

$$\ll \|\alpha\|^2 \|\beta\|^2 \left(\frac{N}{q}\prod_{p|q} p^{h_p}\right)\left(\frac{M}{q[\mathbf{h}]}+1\right)$$
$$\ll \|\alpha\|^2 \|\beta\|^2 \left(\frac{NM}{q^{\frac{1}{2}}}+N\right),$$

as well as

$$\|\beta\|^2 \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M\\(m_1m_2,q)=1}} \overline{\alpha_{m_1}}\alpha_{m_2} \sum_{0<|h|\le\frac{q}{2}} \min\left(\frac{1}{|h|},\frac{N}{q}\right)\prod_{p|q}\left|\mathcal{C}'\big(K_p;(m_1\overline{m_2},s_ph\overline{m_2})\big)\right|$$
$$= \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M\\(m_1m_2,q)=1}} \overline{\alpha_{m_1}}\alpha_{m_2} \sum_{\substack{0<|h|\le\frac{q}{2}\\T[(m_1\overline{m_2},s_ph\overline{m_2})]=\mathbf{h}}} \min\left(\frac{1}{|h|},\frac{N}{q}\right)\prod_{p|q}\left|\mathcal{C}'\big(K_p;(m_1\overline{m_2},s_ph\overline{m_2})\big)\right|$$
$$\ll \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M\\(m_1m_2,q)=1}} |\alpha_{m_1}|\,|\alpha_{m_2}| \sum_{\substack{0<|h|\le\frac{q}{2}\\T[(m_1\overline{m_2},s_ph\overline{m_2})]=\mathbf{h}}} \min\left(\frac{1}{|h|},\frac{N}{q}\right)\prod_{p|q}\left|\mathcal{C}'\big(K_p;(m_1\overline{m_2},s_ph\overline{m_2})\big)\right|$$
$$\ll \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M\\(m_1m_2,q)=1}} |\alpha_{m_1}|\,|\alpha_{m_2}| \sum_{\substack{0<|h|\le\frac{q}{2}\\T[(m_1\overline{m_2},s_ph\overline{m_2})]=\mathbf{h}}} \min\left(\frac{1}{|h|},\frac{N}{q}\right)\prod_{p|q} p^{h_p}$$
$$\ll \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \left(\prod_{p|q} p^{h_p}\right) \sum_{\substack{(a,b)\in\mathbb{F}_{q[\mathbf{h}]}^\times\times\mathbb{F}_{q[\mathbf{h}]}\\ \forall p|q[\mathbf{h}]:\,(a,b)\in\mathbf{H}_{K_p,M}}} \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M\\(m_1m_2,q)=1}} |\alpha_{m_1}|\,|\alpha_{m_2}| \sum_{\substack{0<x\le\frac{q}{2}\\ m_1\overline{m_2}\equiv a \mod q[\mathbf{h}]\\ \pm s_px\overline{m_2}\equiv b \mod q[\mathbf{h}]}} \min\left(\frac{1}{x},\frac{N}{q}\right)$$
$$\ll \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \left(\prod_{p|q} p^{h_p}\right) \sum_{\substack{(a,b)\in\mathbb{F}_{q[\mathbf{h}]}^\times\times\mathbb{F}_{q[\mathbf{h}]}\\ \forall p|q[\mathbf{h}]:\,(a,b)\in\mathbf{H}_{K_p,M}}} \sum_{\substack{\frac{M}{2}\le m_1,m_2\le 2M\\ m_1\overline{m_2}\equiv a \mod q[\mathbf{h}]\\(m_1m_2,q)=1}} \big(|\alpha_{m_1}|^2+|\alpha_{m_2}|^2\big)\left(\frac{\log(q)}{q[\mathbf{h}]}+\frac{N}{q}\right)$$
$$\ll \|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \left(\prod_{p|q} p^{h_p}\right) \sum_{\substack{(a,b)\in\mathbb{F}_{q[\mathbf{h}]}^\times\times\mathbb{F}_{q[\mathbf{h}]}\\ \forall p|q[\mathbf{h}]:\,(a,b)\in\mathbf{H}_{K_p,M}}} \|\alpha\|^2\left(\frac{M}{q[\mathbf{h}]}+1\right)\left(\frac{\log(q)}{q[\mathbf{h}]}+\frac{N}{q}\right)$$
$$\ll \|\alpha\|^2\|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} \left(\prod_{p|q} p^{h_p}\right)\left(\frac{M}{q[\mathbf{h}]}+1\right)\left(\frac{\log(q)}{q[\mathbf{h}]}+\frac{N}{q}\right)$$
$$\ll \|\alpha\|^2\|\beta\|^2 \sum_{\mathbf{h}\in\mathbf{H}} (M+1)\big(q^{\frac{1}{2}}\log(q)+N\big)$$
$$\ll \|\alpha\|^2\|\beta\|^2 \left(Mq^{\frac{1}{2}}\log(q)+q^{\frac{1}{2}}\log(q)+\frac{MN}{q}+\frac{N}{q}\right)$$
$$\ll \|\alpha\|^2\|\beta\|^2 \left(Mq^{\frac{1}{2}}\log(q)+\frac{MN}{q}\right)$$

Hence

$$|T|^2 \ll \|\alpha\|^2\|\beta\|^2\left(Mq^{\frac{1}{2}}\log(q)+\frac{MN}{q}+\frac{MN}{q^{\frac{1}{2}}}+N\right)$$
$$\ll \|\alpha\|^2\|\beta\|^2\left(Mq^{\frac{1}{2}}\log(q)+\frac{MN}{q^{\frac{1}{2}}}+N\right)$$

which yields

$$T \ll \|\alpha\| \, \|\beta\| \, (MN)^{\frac{1}{2}} \Big(\frac{1}{q^{\frac{1}{4}}} + \frac{1}{M^{\frac{1}{2}}} + \frac{q^{\frac{1}{4}} \log^{\frac{1}{2}} q}{N^{\frac{1}{2}}} \Big).$$

This completes the proof of Theorem 6.2.1.

6.3. Proof of Theorem 2.6.3

As explained before, based on the estimates of the type I_2 and type II sums, Theorem 2.6.3 can now be proven completely analogously to [23, Theorem 1.5], the proof being done in section 4 of [23]. Since this part of the proof is completely analytic, replacing the prime p by a squarefree integer q does not make any difference.

7. Applications

As an application of our results, we consider the following proposition which is a generalisation of Corollary 1.13 in [23] and an improvement of [16, Lemmas 6.1, 6.2, 6.3] for $c = q$ squarefree.

Proposition 7.0.1. *For every $0 < \eta < \frac{1}{48}$ there exists $C(\eta)$ such that, for every q squarefree, every $X \geq 2$, and every integer n coprime with q, one has the inequalities*

$$\Big| \sum_{\substack{p<X \\ p \text{ prime}}} \mathrm{Kl}_2(np;q) \log p \Big| \leq C(\eta) X \Big(1 + \frac{q}{X}\Big)^{\frac{1}{12}} q^{-\eta}$$

and

$$\Big| \sum_{\substack{p<X \\ p \text{ prime}}} \mathrm{Kl}_2(n^2p^2;q) e\Big(\frac{2np}{q}\Big) \log p \Big| \leq C(\eta) X \Big(1 + \frac{q}{X}\Big)^{\frac{1}{12}} q^{-\eta}.$$

Proof. By Example 2.3.3 and [22, Section 10.3], we know that

$$K_1(a) = \mathrm{Kl}_2(na;q) \qquad\qquad K_2(a) = \mathrm{Kl}_2(n^2a^2;q) e\Big(\frac{2na}{q}\Big)$$

are irreducible trace functions with conductor ≤ 5 and hence by (q, M)-good and (q, M)-non-exceptional for some absolute constant M. Hence Theorem 2.6.3 is applicable and we obtain

$$\sum_{n<Pq} \Lambda(n) K(n) \ll QP\Big(1 + \frac{1}{P}\Big)^{\frac{1}{12}} q^{1-\eta}$$

for all $0 < \eta < \frac{1}{48}$. Deligne has shown [7, Sommes Trig., (7.1.3)] that

$$|\mathrm{Kl}_m(a;p)| \leq m$$

and hence $K_1(a), K_2(a) \leq 2^{\omega(q)}$. Therefore

$$\begin{aligned}
\sum_{p \leq Pq} K_1(p) \log p &= \sum_{n<Pq} \Lambda(n) K_1(n) - \sum_{2 \leq m \leq \lceil \frac{\log Pq}{\log 2} \rceil} \sum_{p \leq (Pq)^{\frac{1}{m}}} K_1(p^m) \log p \\
&\ll \sum_{n<Pq} \Lambda(n) K_1(n) + q^{\frac{1}{2}+\varepsilon} P \\
&\ll QP\Big(1 + \frac{1}{P}\Big)^{\frac{1}{12}} q^{1-\eta} \\
&= QX\Big(1 + \frac{q}{X}\Big)^{\frac{1}{12}} X^{-\eta},
\end{aligned}$$

for $X = Pq$ and analogously for K_2. □

A. The Kuznetsov Formula

Definition A.0.2. For non-negative integers a, b, c, we define the ***Kloosterman sum*** $S(a, b; c)$ by

$$S(a,b;c) = \sum_{\substack{0 \le x < c \\ (x,c)=1}} e\left(\frac{ax + b\overline{x}}{c}\right).$$

where $\overline{x}$ denotes the inverse of x modulo c.

Proposition A.0.3 (Petersson formula)**.** *For any $n \geq 1$ and $m \geq 1$,*

$$\frac{(k-2)!}{(4\pi)^{k-1}} \sum_{f \in \mathcal{B}_k(D)} \varrho_f(n)\overline{\varrho_f(m)} = \delta(m,n) + 2\pi i^{-k} \sum_{\substack{c>0 \\ D|c}} \frac{1}{c} S(m,n;c) J_{k-1}\left(\frac{4\pi\sqrt{mn}}{c}\right).$$

Proof. This is Proposition 14.5 in [17]. Note that their $\mathcal{F}$ is our $\mathcal{B}_k(D)$. □

Proposition A.0.4 (Trivial bound for Kloosterman sums)**.** *The trivial bound is*

$$|S(a,b;c)| \leq c.$$

Proposition A.0.5 (Weil's bound for Kloosterman sums)**.** *Let $a, b, c \in \mathbb{Z}$, c positive. Then*

$$|S(a,b;c)| \leq \tau(c)\sqrt{(a,b,c)}\sqrt{c}$$

where τ denotes the divisor function and (a, b, c) the greatest common divisor of a, b and c.

Proposition A.0.6 (Twisted multiplicativity of Kloosterman sums)**.** *If $(c, d) = 1$, then*

$$S(a,b;cd) = S(a\overline{c}, b\overline{c}; d) S(a\overline{d}, b\overline{d}; c),$$

where $\overline{c}$ and $\overline{d}$ denote integers such that $c\overline{c} \equiv 1 \mod d$ and $d\overline{d} \equiv 1 \mod c$.

A proof of Proposition A.0.5 can for example be found in [17, Corollary 11.12]. Proposition A.0.6 is Equation (1.59) in [17].

The Kuznetsov formula is a generalization of the Petersson formula. The following statement can be found in [22], Section 3.1.5.

Theorem A.0.7 (Kuznetsov formula)**.** *Let $\phi\colon [0, \infty[\longrightarrow \mathbb{C}$ be a smooth function satisfying*

$$\phi(0) = \phi'(0) = 0, \qquad \frac{d^j}{dx^j}\phi(x) \ll_\varepsilon (1+x)^{-2-\varepsilon} \text{ for } 0 \leq j \leq 3.$$

Let

$$\dot{\phi}(k) = i^k \int_0^\infty J_{k-1}(x)\phi(x)\frac{dx}{x},$$
$$\tilde{\phi}(t) = \frac{i}{2\sinh(\pi t)} \int_0^\infty (J_{2it}(x) - J_{-2it}(x))\phi(x)\frac{dx}{x},$$

$$\check{\phi}(t) = \frac{2}{\pi}\cosh(\pi t)\int_0^\infty K_{2it}(x)\phi(x)\frac{dx}{x}$$

be Bessel transforms. Then for positive integers m, n we have the following trace formula due to Kuznetsov:

$$\Delta_{D,\phi}(m,n) = \sum_{\substack{c>0\\ D|c}} \frac{1}{c} S(m,n;c)\phi\left(\frac{4\pi\sqrt{mn}}{c}\right)$$

where

$$\Delta_{D,\phi}(m,n) := \sum_{\substack{k>0\\ k\equiv 0 \mod 2}} \sum_{g\in\mathcal{B}_k(D)} \dot{\phi}(k)\frac{(k-1)!}{\pi(4\pi)^{k-1}}\overline{\varrho_g(m)}\varrho_g(n) + \sum_{g\in\mathcal{B}(D)} \tilde{\phi}(t_g)\frac{4\pi}{\cosh(\pi t_g)}\overline{\varrho_g(m)}\varrho_g(n)$$
$$+ \sum_{\chi}\sum_{g\in\mathcal{B}(\chi)} \int_{-\infty}^{\infty} \tilde{\phi}(t)\frac{1}{\cosh(\pi t)}\overline{\varrho_g(m,t)}\varrho_g(n,t)dt.$$

Definition A.0.8 (Test function $\phi_{a,b}$)**.** Let $a, b \in \mathbb{Z}$ such that $2 \le b < a$, b is odd and $a - b \equiv 0 \mod 2$. Then we define

$$\phi_{a,b}(x) = i^{b-a}J_a(x)x^{-b}.$$

By [3, (2.21)], we get the following proposition (see also [22, p. 604]):

Proposition A.0.9. *We have*

$$\dot{\phi}_{a,b}(k) = \frac{b!}{2^{b+1}\pi}\prod_{j=0}^{b}\left(\left(\frac{(1-k)i}{2}\right)^2 + \left(\frac{a+b}{2} - j\right)^2\right)^{-1} \asymp_{a,b} \pm k^{-2b-2},$$
$$\tilde{\phi}_{a,b}(t) = \frac{b!}{2^{b+1}\pi}\prod_{j=0}^{b}\left(t^2 + \left(\frac{a+b}{2} - j\right)^2\right)^{-1} \asymp_{a,b} (1+|t|)^{-2b-2}.$$

In particular

$$\begin{cases} \dot{\phi}_{a,b}(k) > 0 & \text{for } 2 \le k \le a-b, \\ (-1)^{(k-(a-b))/2}\dot{\phi}_{a,b}(k) > 0 & \text{for } a-b < k \le a+b, \\ \dot{\phi}_{a,b}(k) > 0 & \text{for } a+b < k, \\ \tilde{\phi}_{a,b}(t) > 0 & \text{for } t \in \mathbb{R} \cup (-i/4, i/4). \end{cases}$$

B. Some Auxiliary Results

Proposition B.0.10 (Hecke relations)**.** *Let f be a Hecke eigenform. Then for $(m,D)=1$ and any $n\geq 1$, we have*

$$\lambda_f(m)\varrho_f(n)=\sum_{d|(m,n)}\varrho_f\Big(\frac{mn}{d^2}\Big),$$

and moreover, these relations hold for all m,n if f is a newform, with an additional factor $\chi_0(d)$, where χ_0 denotes the principal Dirichlet character to modulus D. (Recall that λ_f are the Hecke eigenvalues and ϱ_f are the Fourier coefficients.

Proposition B.0.11. *Let g be a Hecke eigenform and let λ_g denote its Hecke eigenvalues. Then, for primes $\ell_1\neq\ell_2$, we have that*

$$\lambda_g(\ell_1)\lambda_g(\ell_2)=\lambda_g(\ell_1\ell_2).$$

Theorem B.0.12 (Large Sieve Inequality)**.** *For any sequence of complex numbers $(a_n)_{0\leq n\leq N}$, we have*

$$\sum_{f\in\mathcal{B}_k(D)}\Big|\sum_{n\leq N}a_n\varrho_f(n)\Big|^2\ll_k\Big(1+\frac{N}{q}\Big)\|a\|^2=\Big(1+\frac{N}{q}\Big)\sum_{n=0}^{N}|a_n|^2$$

where the implied constant depends only on the weight k.

Proof. This is Theorem 7.26 in [17]. Recall, that for $f\in\mathcal{B}_k(D)$, we write the Fourier expansion at ∞ in the form

$$f(z)=\sum_{n\geq 1}n^{\frac{k-1}{2}}\varrho_f(n)e(nz),$$

whereas in [17, page 187], the Fourier expansion is written in the form

$$f(z)=\sum_{n\geq 1}a_f(n)e(nz).$$

Furthermore, where we denote an orthonormal (with respect to the Petersson norm) basis of $\mathcal{S}_k(D)$ by $\mathcal{B}_k(D)$, in [17] such an orthonormal basis is denoted by $\mathcal{F}$. At this point there occurs no normalization issue, as our definition of the Petersson norm (Definition 2.4.10) coincides with the one in [17] (equation (14.11) on page 357). Hence, for $f\in\mathcal{B}_k(D)$, the normalized Fourier coefficient $\psi_f(n)$ (equation (7.43) in [17]) becomes

$$\psi_f(n)=\left(\frac{q(k-2)!}{(4\pi n)^{k-1}}\right)^{\frac{1}{2}}a_f(n)=\left(\frac{q(k-2)!}{(4\pi)^{k-1}}\right)^{\frac{1}{2}}\varrho_f(n).$$

Hence, the statement of [17, Theorem 7.26] reads

$$\frac{q(k-2)!}{(4\pi)^{k-1}}\sum_{f\in\mathcal{B}_k(D)}\Big|\sum_{n\leq N}a_n\varrho_f(n)\Big|^2\ll(q+N)\|a\|^2$$

from where the theorem follows. □

Proposition B.0.13 (Duke, Friedlander and Iwaniec). *Let $f \in \mathcal{B}(D)$. Then for any $x \geq 1$ and any $\varepsilon > 0$,*

$$\sum_{n \leq x} |\lambda_f(n)|^2 \ll_\varepsilon x(xD(1+|t_f|))^\varepsilon.$$

where $\frac{1}{4} + t_f^2$ denotes the Laplace eigenvalue of f and the $\lambda_f(n)$'s denote the Hecke eigenvalues of f.

Proof. This is Proposition 19.6 in [9]. Note that in [9], the Laplace eigenvalue is written $s_f(1-s_f) = \frac{1}{4} - t_f^2$. Hence

$$s_f = \pm t_f i - \frac{1}{2}$$

and hence

$$|s_f| = \left|\pm t_f i - \frac{1}{2}\right| \leq |t_f| + 1.$$

So, for any $x \geq 1$ and any $\varepsilon > 0$,

$$\sum_{n \leq x} |\lambda_f(n)|^2 \ll_\varepsilon x(xD\,|s_j|)^\varepsilon \leq x(xD(1+|t_f|))^\varepsilon.$$

□

Proposition B.0.14 (Deshouillers and Iwaniec). *Let $K \geq 1$, $N \geq \frac{1}{2}$ and $\varepsilon > 0$ be real numbers, (a_n) a sequence of complex numbers and $\mathfrak{a}$ a cusp of $\Gamma_0(D)$; each of the three expressions*

$$\sum_{\substack{2 \leq k \leq K \\ k \text{ even}}} \frac{(k-1)!}{(4\pi)^{k-1}} \sum_{1 \leq j \leq \theta_k(q)} \left| \sum_{N < n \leq 2N} a_n n^{-\frac{k-1}{2}} \psi_{jk}(\mathfrak{a}, n) \right|^2$$

$$\sum_{\substack{g \in \mathcal{B}(D) \\ |t_f| \leq K}} \frac{1}{\cosh(\pi t_f)} \left| \sum_{N < n \leq 2N} a_n \rho_{f\mathfrak{a}}(n) \right|^2$$

$$\sum_{\mathfrak{c}} \int_{-K}^{K} \left| \sum_{N < n \leq 2N} a_n n^{ir} \varphi_{\mathfrak{ca}n}\Big(\frac{1}{2} + ir\Big) \right|^2 dr$$

is majorized up to a constant depending on ε at most by

$$(K^2 + (w, \frac{D}{w})D^{-1}N^{1+\varepsilon}) \sum_{n \leq N} a_n^2,$$

where $\rho_{f\mathfrak{a}}(n)$ denotes the n-th Fourier coefficient at the cusp $\mathfrak{a}$.

Proof. See Theorem 2 in [8]. □

Lemma B.0.15. *For every $g \in \mathcal{B}(D)$, we have that t_f is either real or purely imaginary with $-\frac{1}{2} < it_f < \frac{1}{2}$. Hence,* $\cosh(\pi t_f) > 0$.

Proof. See remark after Theorem 2 in [8]. □

Corollary B.0.16. *For all $g \in \mathcal{B}(D)$ with $|t_g| \geq \frac{1}{2}$, we have that* $\cosh(\pi t_g) > \frac{5}{2}$.

Theorem B.0.17 (***Deligne's bound*** on Hecke eigenvalues of holomorphic cusp forms (or unitary Eisenstein series))**.** *For a primitive cusp form $f \in \mathcal{S}_k(D)$, we have*

$$|\lambda_f(n)| \leq d(n) \ll_\varepsilon n^\varepsilon,$$

where $\lambda_f(n)$ denotes the Hecke eigenvalue of f and $d(n)$ denotes the divisor function.

Remark B.0.18. This theorem is easy for coefficients of Eisenstein series, but very very deep for general holomorphic cusp forms (based on the Riemann hypothesis over finite fields).

Theorem B.0.17 is also called the ***Ramanujan-Petersson conjecture for modular forms***, or simply the ***Ramanujan-Petersson bound***. The conjecture is still open for Maass forms.

Proof. See, e.g., equation (14.54) in [17]. □

Theorem B.0.19 (Poisson summation formula)**.** *Suppose that both f, $\hat{f}$ are in $L^1(\mathbb{R})$ and have bounded variation. Further suppose that $v \in \mathbb{R}^+$ and $u \in \mathbb{R}$. Then*

$$\sum_{m\in\mathbb{Z}} f(vm+u) = \frac{1}{v}\sum_{n\in\mathbb{Z}} \hat{f}\Big(\frac{n}{n}\Big)e\Big(\frac{un}{v}\Big),$$

where both series converge absolutely.

Proof. This is Theorem 4.4 and formula (4.24) in [17]. □

Theorem B.0.20 (Poisson summation formula in several variable)**.** *Suppose f is in the Schwartz class $\mathcal{S}(\mathbb{R}^\ell)$. Then*

$$\sum_{m\in\mathbb{Z}^\ell} f(m) = \sum_{n\in\mathbb{Z}^\ell} \hat{f}(n).$$

Furthermore, for $v \in \mathbb{R}^+$ and $u \in \mathbb{R}^\ell$, we have

$$\sum_{m\in\mathbb{Z}^\ell} f(vm+u) = \frac{1}{v^\ell}\sum_{n\in\mathbb{Z}^\ell} \hat{f}\Big(\frac{n}{v}\Big)e\Big(\frac{1}{v}\langle u,n\rangle\Big).$$

Proof. The first equality is Theorem 4.5 in [17]. The second equation follows by applying the first equation to $h(m) = f(vm+u)$ and computing

$$\hat{h}(n) = \int_{\mathbb{R}^\ell} h(\tilde{m})e(-\langle\tilde{m},n\rangle)d\tilde{m} = \int_{\mathbb{R}^\ell} f(v\tilde{m}+u)e(-\langle\tilde{m},n\rangle)d\tilde{m}$$

which is by setting $m = v\tilde{m}+u$

$$\begin{aligned} &= \frac{1}{v^\ell}\int_{\mathbb{R}^\ell} f(m)e\Big(-\frac{1}{v}\langle m-u,n\rangle\Big)dm \\ &= \frac{1}{v^\ell}e\Big(\frac{1}{v}\langle u,n\rangle\Big)\int_{\mathbb{R}^\ell} f(m)e\Big(-\langle m,\frac{n}{v}\rangle\Big)dm = \frac{1}{v^\ell}e\Big(\frac{1}{v}\langle u,n\rangle\Big)\hat{f}\Big(\frac{n}{v}\Big). \end{aligned}$$

□

The next theorem is Lemma 5.2 of an earlier version of F-K-M.

Theorem B.0.21. *Let* $Q(X,Y) = aX^2 + bXY + cY^2$ *be an integral quadratic form with* $ab \neq 0$, $a > 0$ *and discriminant* Δ. *For* $n \geq 1$ *and* $X \geq 1$, *the number* $N_X(n)$ *of integral solutions to the equation*

$$Q(x, y) = n,$$

such that $\max(|x|, |y|) \leq X$ *satisfies*

$$N_X(n) \ll (nX |ac| (|b| + 1))^{\varepsilon},$$

for any $\varepsilon > 0$, *where the implied constant depends only on* ε.

Bibliography

[1] V. Blomer, É. Fouvry, E. Kowalski, Ph. Michel, and D. Milićević. On moments of twisted L-functions. *American J. of Math.*, to appear.

[2] V. Blomer and G. Harcos. Hybrid bounds for twisted L-functions. *J. reine und angew. Mathematik*, 621:53–79, 2008.

[3] V. Blomer, G. Harcos, and Ph. Michel. Bounds for modular L-functions in the level aspect. *Ann. Sci. École Norm. Sup. (4)*, (5)40:697–740, 2007.

[4] J.H. Bruinier, G. van der Geer, G. Harder, and D. Zagier. *The 1-2-3 of Modular Forms.* Springer, 2008.

[5] V.A. Bykovski. A trace formula for the scalar product of hecke series and its applications. *J. Math. Science*, 89:915–932, 1998.

[6] J.B. Conrey and H. Iwaniec. The cubic moment of central values of automorphic L-functions. *Ann. of Math.*, 151:1175–1216, 2000.

[7] P. Deligne. *Cohomologie étale, S.G.A.*$4\frac{1}{2}$, volume 569 of *L.N.M.* Springer, 1977.

[8] J-M. Deshouillers and H. Iwaniec. Kloosterman sums and Fourier coefficients of cusp forms. *Invent. math.*, 70:219–288, 1982.

[9] W. Duke, J. B. Friedlander, and H. Iwaniec. The subconvexity problem for Artin L-functions. *Invent. math.*, 149:489–577, 2002.

[10] W.D. Duke, J. Friedlander, and H. Iwaniec. Bounds for automorphic L-functions. *Invent. math.*

[11] É. Fouvry, E. Kowalski, and Ph. Michel. On the exponent of distribution for the ternary divisor function. *Mathematika*, 61:121–144, 2015.

[12] I.S. Gradshteyn and I.M. Ryzhik. *Table of Integrals, Series and Products.* Academic Press, seventh edition, 2007.

[13] H. Iwaniec. Fourier coefficients of modular forms of half-integral weight. *Invent. math.*, 87:385–401, 1987.

[14] H. Iwaniec. *Introduction to the spectral theory of automorphic forms.* Biblioteca de la Revista Matematica Iberoamericana. Revista Matematica Iberoamericana, 1995.

[15] H. Iwaniec. *Topics in classical automorphic forms*, volume 17 of *Grad. Studies in Math.* A.M.S., 1997.

[16] H. Iwaniec, W. Luo, and P. Sarnak. Low lying zeros of families of L-functions. *Publ. Math. Inst. hautes Études Sci.*, 91:55–131, 2000.

[17] Henryk Iwaniec and Emmanuel Kowalski. *Analytic Number Theory*. American Mathematical Society, 2004.

[18] N.M. Katz. *Gauss sums, Kloosterman sums and monodromy groups*, volume 116 of *Annals of Math. Studies*. Princeton University Press, 1988.

[19] N.M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Math. Studies*. Princeton University Press, 1990.

[20] E. Kowalski. Trace functions over finite fields and applications, 2014. Available at www.math.ethz.ch/∼kowalski.

[21] E. Kowalski, O. Robert, and J. Wu. Small gaps in coefficients of L-functions ond $\mathfrak{B}$-free numbers in small intervals. *Rev. Mat. Iberoamericana*, 23:281–326, 2007.

[22] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. Algebraic twists of modular forms and hecke orbits. *eprint arXiv:1207.0617*, 2012.

[23] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. Algebraic trace functions over the primes. *Duke Math. J.*, (9)163:1683–1736, 2014.