TOPICS IN ANALYTIC NUMBER THEORY

FARZAD ARYAN
Bachelor of Science, Bahonar University of Kerman, 2006
Master of Science, Iran university of science and technology, 2009
Master of Science, University of Montreal, 2012

A Thesis
Submitted to the School of Graduate Studies
of the University of Lethbridge
in Partial Fulfillment of the
Requirements for the Degree

DOCTOR OF PHILOSOPHY

Department of Mathematics and Computer Science
University of Lethbridge
LETHBRIDGE, ALBERTA, CANADA

TOPICS IN ANALYTIC NUMBER THEORY

FARZAD ARYAN

Date of Defence: January 28, 2016

Dr. Nathan Ng		
Supervisor	Associate Professor	Ph.D.
Dr. Amir Akbary		
Committee Member	Professor	Ph.D.
Dr. Habiba Kadiri		
Committee Member	Assistant Professor	Ph.D.
Dr. Pascal Ghazalian		
Committee Member	Associate Professor	Ph.D.
Dr. Youness Lamzouri, York University,		
External examiner	Assistant Professor	Ph.D.
Dr. Hadi Kharaghani		
Chair, Thesis Examination Committee	Professor	Ph.D.

Dedication

To the loving memories of my father

Yahya Aryan

and my Mother

Zahra Sadoughi

whom I miss and love for always.

Abstract

In this thesis, we investigate three topics belonging to the probabilistic, classical and modern branches of analytic number theory.

Our first result concerns the probabilistic distribution of squares modulo a composite number, and of tuples of reduced residues, in short intervals. We obtain variance upper bounds generalizing those of Montgomery and Vaughan, as well as new lower bounds.

Our second work, joint with Nathan Ng, concerns the estimation of discrete mean values of Dirichlet polynomials, where summation is over the zeros of an L-function attached to an automorphic representation. Conditionally on strong bounds on autocorrelations of the coefficients of L-functions, a corollary of our results is that the gaps between consecutive zeros of the Riemann zeta function are infinitely often smaller than half of the average gap.

Our last work concerns the additive and quadratic divisor problem. We study shifted convolution sums for the divisor function, Fourier coefficients of a cusp form and the representation function of integers as sums of two squares. For convolution sums of a certain type, we improve several estimates available in the literature, by expanding the delta-method of Duke, Friedlander and Iwaniec. Also by using a smooth variant of Dirichlet hyperbola method, we improve the error term obtained by Duke, Friedlander and Iwaniec in the quadratic divisor problem.

Acknowledgments

Contents

List of Tables

List of Figures

Chapter 1

Introduction

This thesis consists of three main parts, which are related to the following branches of number theory.

1. Probabilistic number theory.

2. Classical analytic number theory.

3. Modern analytic number theory.

Here we will give a brief introduction to each of these branches and I will mention how my PhD thesis is connected to them.

1.1   Probabilistic number theory

Probabilistic number theory studies the probability distribution of arithmetic objects. Frequently the object under consideration is a sequence or points on certain curve that has arithmetic significance. Sequences such as prime numbers, Fourier coefficients of modular forms, and Heegner points on a modular curves have been extensively studied. Before giving some examples we review some basic facts from probability.

We call the triple $(\Omega, \mathcal{F}, \mathcal{P})$ a probability space when Ω is the set of possible outcomes, $\mathcal{F}$ is a sigma-algebra on Ω and $\mathcal{P}$ is a measure on $\mathcal{F}$ such that $\mathcal{P}(\Omega) = 1$. A random variable X is a measurable function defined on Ω. We now define the following probabilistic objects.

1. Expectation of X:

$$\mathbf{E}(X) := \int_{\Omega} X d\mathcal{P}. \tag{1.1}$$

2. Variance of X:

$$\mathbf{Var}(X) := \int_{\Omega} (X - \mathbf{E}(X))^2 d\mathcal{P}. \tag{1.2}$$

3. Distribution of a random variable: We say that $f_{den}(x)$ is the probability density function for the random variable X, and we identify the distribution of X with $f_{den}(x)$, if

$$\mathcal{P}(a \leq X \leq b) = \int_{a}^{b} f_{den}(x) dx. \tag{1.3}$$

In studying a sequence one of the first questions that comes to mind concerns the average of the sequence on an interval. More precisely, let $f(n)$ be a sequence and $[a,b]$ an interval. Let

$$\overline{f}_{[a,b]} := \frac{\sum_{a \leq n \leq b} f(n)}{b-a} \tag{1.4}$$

denote the average of f on the interval $[a,b]$. For example if we set $f(n) = \mathbf{1}_P(n)$ to be the characteristic function of the primes, then $\overline{\mathbf{1}}_{P_{[1,x]}}$ can be considered as the "probability" of a random integer in the interval $[1,x]$ being prime. Studying asymptotic estimates of $\overline{\mathbf{1}}_{P_{[1,x]}}$ was one of the main problems that started classical analytic number theory. Gauss conjectured that the "probability" of a random integer smaller than x being prime is $(\log x)^{-1}$. i.e.

$$\overline{\mathbf{1}}_{P_{[1,x]}} \sim \frac{1}{\log x}. \tag{1.5}$$

However he could not prove this result. The first major result toward a proof of Gauss's conjecture was obtained by Chebyshev. He proved that

$$\frac{0.92129}{\log x} < \overline{\mathbf{1}}_{P_{[1,x]}} < \frac{1.10555}{\log x}.$$

Finally, the conjecture of Gauss was proved by Hadamard and de la Vallée-Poussin in 1896.

After finding an average of a sequence the next question that comes to mind concerns how this sequence is distributed around the average. To study this we use the variance of the sequence. Assume that we are looking at the distribution of f in the interval $[1,x]$ and consider the following sum:

$$\frac{1}{x} \sum_{m \leq x} \Big(\sum_{n \in [m,m+h]} f(n) - \overline{f}_{[1,x]} h \Big)^{2k}. \tag{1.6}$$

Evaluating the above when $k = 1$ gives the variance of the distribution. When we speak of the higher moments of the distribution of f we refer to the above with $k > 1$. Finding an upper bound for the variance when f is the characteristic function of the primes would prove the strong statement

$$\sum_{p_n < x} (p_{n+1} - p_n)^2 \ll x(\log x)^{3+\varepsilon} \tag{1.7}$$

on average gaps between primes. However proving such a bound unconditionally seems very deep and out of reach of current methods. This difficulty led Erdős to propose a similar conjecture for the average gaps between the reduced residues. The set of reduced residues modulo an integer q is

$$\{1 \leq n \leq q \mid (n,q) = 1\} = \{1 = a_1 < \ldots < a_{\phi(n)} = q-1\}. \tag{1.8}$$

We will denote the characteristic function of reduced residues modulo q with $k_q(n)$. Erdős conjectured that

$$\sum_{i=1}^{\phi(q)} (a_{i+1} - a_i)^2 \ll q^2/\phi(q),$$

where $\phi(.)$ is the Euler totient function.

Erdős' conjecture was settled by Montgomery and Vaughan, who gave an optimal estimate

for all moments of the distribution of reduced residues.

Theorem 1.1 (Montgomery and Vaughan [60]). *Let k be a fixed natural number. Then*

$$\sum_{n=0}^{q-1} \left(\sum_{m=1}^{h} k_q(n+m) - h\frac{\phi(q)}{q} \right)^k \ll q(h\frac{\phi(q)}{q})^{k/2} + h\phi(q).$$

In the author's master's thesis [3], motivated by prime s-tuples conjecture, we studied the distribution of s-tuples of reduced residues. Let $\mathcal{D} = \{h_1, h_2, \cdots, h_s\}$ and $\nu_p(\mathcal{D})$ be the number of distinct elements in $\mathcal{D}$ mod p. We call $\mathcal{D}$ *admissible* if $\nu_p(\mathcal{D}) < p$ for all primes p. Before defining s-tuples of reduced residues we state the prime s-tuples conjecture.

Conjecture 1.2. There exist infinitely many numbers m such that for all $h \in \mathcal{D}$, $m+h$ is a prime number.

This conjecture is challenging and even the case $s = 2$ is unsolved at the moment. Prime numbers $m + h_i$ for $1 \leq i \leq s$ are called a s-tuples of primes. Similarly, we call $a + h_1, \ldots, a + h_s$ an *s-tuple of reduced residues* if they are each coprime with q. In the author's master's thesis, by obtaining an upper bound on the moments of the distribution of s-tuples of reduced residues, we proved the analogue of Erdős' conjecture for s-tuples of reduced residues. However the upper bounds obtained on the moments of the distribution of reduced residues were not optimal. In this thesis we will give an optimal upper bound.

Squares form another interesting sequence, which has been the subject of much study. Obviously when we consider $\{s^2\}$ in $\mathbb{Z}$ the sequence is far from evenly distributed. However this changes when one reduces squares modulo an integer. A number s is called a *square modulo a prime p* if it is a reduced residue of a square in $\mathbb{Z}$. We call an integer a *square modulo a square free number q* if it is a square modulo each prime factor of q. In this thesis we will study the variance of the distribution of squares modulo a square free composite number q. We will obtain bounds on the variance that are very close to the optimal bound.

Theorem 1.3 (Aryan)**.** *Let $h \gg 2^{\omega(q)}$ be a natural number and $X_h(n) = \#\{s \in [n, n+h] :$ s is a $\square$ modulo q\}, be a random variable. We have*

$$\mathbf{Var}(X_h) \leq \mathbf{E}(X_h)^{1+\varepsilon}.$$

From this theorem we deduce the following result concerning consecutive squares modulo q.

Corollary 1.4. *Let s_i be the squares modulo q in increasing order. Then*

$$\frac{1}{q} \sum_{s_i < q} (s_{i+1} - s_i)^2 \ll 2^{\omega(q)} P(\log q) \prod_{p|q} \left(1 + \frac{1}{\sqrt{p}}\right).$$

We finish this part by stating a famous result about another interesting arithmetic sequence. Let $\omega(n)$ denote the number of prime divisors of n. The average of ω in the interval $[1, x]$ is about $\log \log x$. One of the celebrated results in probabilistic number theory, due to Erdős and Kac, gives the distribution of ω.

Theorem 1.5 (Erdős-Kac)**.** *For any positive integer n and any real number a, b we have*

$$\lim_{x \longrightarrow \infty} \frac{1}{x} \left| \left\{ 1 \leq n \leq x \mid a \leq \frac{\omega(n) - \log \log n}{\sqrt{\log \log n}} \leq b \right\} \right| = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-x^2/2} dx. \qquad (1.9)$$

1.2 Classical Analytic Number Theory

Classical analytic number theory started by Euler, Dirichlet and Riemann. Consider the Riemann zeta function defined for $\Re(s) > 1$ by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \qquad (1.10)$$

The zeta function has an Euler product

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \qquad (1.11)$$

5

on $\Re(s) > 1$ and an analytic continuation to the whole complex plane with a simple pole of residue 1 at $s = 1$. Using the Euler product of the zeta function, Euler showed that there exist infinitely many prime numbers. Riemann, in his only paper in Number Theory, showed that there exists a close connection between the zeros of the zeta function and the distribution of prime numbers. In fact from his work one can show that to prove (1.5) it is enough to show that $\zeta(s) \neq 0$ for $\Re(s) = 1$. One of the important parts of his paper was the functional equation he found for the zeta function.

Functional Equation for the Riemann zeta function. Let $\Gamma(s)$ denote the Gamma function. Then

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s) \zeta(1-s). \tag{1.12}$$

Note that the above functional equation says that $\zeta(s) = 0$ when s is equal to a negative even integer. These zeros are known as the trivial zeros of the Riemann zeta function. Also, the functional equation shows a symmetry between the values of the zeta function with respect to the line $\Re(s) = 1/2$. Perhaps this was one of the reasons Riemann made a conjecture about the location of the zeros of the zeta function.

The Riemann hypothesis. All the non-trivial zeros of the Riemann zeta function are located on the line

$$\Re(s) = \tfrac{1}{2}.$$

The Riemann hypothesis is known as the most famous unsolved problem in mathematics. The connection with the distribution of prime numbers comes from the Riemann's Explicit Formula. Let

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \\ 0 & \text{otherwise.} \end{cases}$$

We have that

$$\psi(x) := \sum_{n \leq x} \Lambda(n) = x + \sum_{\zeta(\rho)=0} \frac{x^\rho}{\rho} + O(1). \tag{1.13}$$

Now if we assume the Riemann hypothesis we have that all the zeros of ζ are of the form $1/2 + it_\rho$, and therefore we can get

$$\psi(x) = x + O(x^{1/2+\varepsilon}). \tag{1.14}$$

Note that the prime number theorem, (1.5), is equivalent to a much weaker estimate:

$$\psi(x) = x + o(x). \tag{1.15}$$

Although Riemann did not prove the prime number theorem, his paper had a profound impact on number theory. Another important contribution to this field was made by Dirichlet. He proved that there exist infinitely many prime numbers in an arithmetic progression(i.e. of the form $an + b$ where $(a,b) = 1$). Dirichlet's method was based on the properties of Dirichlet L-functions. Let $\chi(.)$ be a completely multiplicative function from $\mathbb{Z}/q\mathbb{Z}$ to $\mathbb{C}$. We define the Dirichlet L-function associated to χ for $\Re(s) > 1$ by

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{1.16}$$

The main ingredient of his proof was the assertion $L(1,\chi) \neq 0$. After Dirichlet, a major development came with the proof of the prime number theorem by Hadamard and de la Vallée-Poussin. They showed that $\zeta(s) \neq 0$ for $\Re(s) = 1$. To this day there have been only minor improvements of their result, which shows that improving the error term in the prime number theorem is a very hard problem.

Another major development was made by Montgomery while he was working on the distribution of the zeros of the Riemann zeta function. Let γ_i denote the zeros of the Rie-

7

mann zeta function on the critical line. Montgomery's work suggest that, assuming the Riemann hypothesis, the distribution of the zeros of the zeta function has a certain statistical property. It has been pointed out to him by physicist Freeman Dyson that the distribution he found is the same as the pair correlation distribution for the eigenvalues of a random Hermitian matrix.

Conjecture 1.6 (Montgomery's Pair Correlation Conjecture). For a fixed interval (a, b) we have

$$\lim_{T \to \infty} \frac{\left| \{ (\gamma, \gamma') | \frac{\log T}{2\pi} (\gamma - \gamma') \in (a, b) \} \right|}{\frac{T}{2\pi} \log T} = \int_a^b \left(1 - \frac{\sin(\pi u)}{\pi u} \right) du \qquad (1.17)$$

where γ, γ' denote the imaginary parts of the zeros of the zeta function on the critical line.

By the zero counting function we know that the zeta function has about $T \log T / 2\pi$ zeros in the critical strip with imaginary part between 0 and T. This tells us that the average gap between the zeros of the zeta function is about $2\pi / \log T$. Montgomery's Pair Correlation Conjecture implies that we can find infinitely many tuples of zeros (γ, γ') such that $|\gamma - \gamma'| < c 2\pi / \log T$, for every $c > 0$. From his work on the pair correlation Montgomery was able to deduce that $c < 0.68$. Many authors improved 0.68 to a number slightly bigger than 0.51. It seems very challenging to prove unconditionally that one can take $c < 0.5$. In this thesis by assuming conjectures on the shifted convolution sums of Liouville's function, we show that $c < 0.4999$.

Theorem 1.7 (Aryan and Ng). *Assume the Riemann hypothesis, and Chowla's conjectures ((3.33) and (3.34)) on the shifted convolution sums of the Liouville's function. Then there exist infinitely many tuples $(\frac{1}{2} + i\gamma, \frac{1}{2} + i\gamma')$ of zeros of the Riemann zeta function with*

$$|\gamma - \gamma'| < 0.4999 \frac{2\pi}{\log T}.$$

To explain our work let us first state Montgomery and Vaughan's mean value theorem for Dirichlet polynomials

Theorem 1.8 (Montgomery and Vaughan). *Let $\{a(n)\}$ and $\{b(n)\}$ be two sequences of complex numbers. For any real number $T > 0$, we have*

$$\int_0^T \left(\sum_{n=1}^{\infty} a(n)n^{-it} \right) \left(\sum_{n=1}^{\infty} b(n)n^{it} \right) dt \qquad (1.18)$$
$$= \sum_{n=1}^{\infty} a(n)b(n) + O\left(\left(\sum_{n=1}^{\infty} na(n) \right)^{\frac{1}{2}} \left(\sum_{n=1}^{\infty} nb(n) \right)^{\frac{1}{2}} \right).$$

Note that if $\{a(n)\}$ and $\{b(n)\}$ are supported on an interval of length $o(T)$ then (1.18) become an asymptotic. Goldston and Gonek [28] considered this theorem for Dirichlet polynomials of arbitrary length. Their work shows that when support of $\{a(n)\}$ and $\{b(n)\}$ are in intervals with length larger than T then it is crucial to consider the shifted convolution sums of $a(n)$ and $b(n)$. In other words to get a result in this case we need an estimate on

$$\sum_{n<x} a(n)b(n+h).$$

In our work we considered a discrete version of the above theorem. More precisely we studied

$$\sum_{L(\rho)=0} \omega(\rho)A(\rho)B(1-\rho) \qquad (1.19)$$

where $L(s)$ is an L-function, $\omega(s)$ is an entire weight and

$$A(s) = \sum_{n \leq N}^{\infty} a(n)n^{-s} \text{ and } B(s) = \sum_{n \leq M}^{\infty} b(n)n^{-s}.$$

We derived a formula for (1.19) in terms of shifted convolution sums involving $a(n)$, $b(n)$, and $\Lambda_L(n)$, where $\Lambda_L(n)$ is defined by

$$\frac{L'}{L}(s) = -\sum_{n=1}^{\infty} \frac{\Lambda_L(n)}{n^s}.$$

For the application to the small gaps between the zeros of the Riemann zeta function we used the choice $a(n) = b(n) = \lambda(n)$, where $\lambda(n)$ is Liouville's function.

9

1.3 Modern Analytic Number Theory

If we consider the Euler product of the Riemann zeta function or Dirichlet L-functions,

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

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

we observe a similarity between them. Note that each Euler factor is a degree one polynomial in terms of p^{-s}. A question arises regarding L-functions whose Euler products involves higher degree polynomials. This is a place where we enter the boundaries of modern analytic number theory. As an example consider Ramanujan's Δ function:

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n, \quad q = e^{2\pi i z}. \tag{1.20}$$

The L-function associated to Δ for $\Re(s) > 13/2$ is

$$\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s},$$

and it has the Euler product

$$\prod_p \left(1 - \tau(p) p^{-s} + p^{k-1-2s}\right)^{-1}. \tag{1.21}$$

The function $\Delta(z)$ is a holomorphic cusp form of weight 12 and level 1. Cusp forms are special types of modular forms.

Definition 1.9 (Modular form of weight k and level 1)**.** Let

$$SL(2,\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{Z},\ ad - bc = 1 \right\}$$

A modular form of weight k and level 1 is a complex valued function defined on the upper half plane $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ that satisfies the following.

1- f is a holomorphic function on the upper half plane.

2- For any $z \in \mathbb{H}$ and all matrices in $SL(2, \mathbb{Z})$, we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z). \tag{1.22}$$

3- f is holomorphic at the cusp at ∞.

Studying modular forms is very important in mathematics. For example they played important role in proving Fermat's last theorem. They also, among many other applications, are used in proving the equidistribution of certain points on modular curves.

Let

$$\Gamma_0(q) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, \mathbb{Z}) \mid c \equiv 0 \bmod q \right\}$$

and

$$\Gamma(q) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, \mathbb{Z}) \mid c \equiv b \equiv 0, \ a \equiv d \equiv 1 \bmod q \right\}.$$

These are known as congruence subgroups. Now if we have a modular form that satisfies the functional equation (1.22) for all matrices in $\Gamma(q)$ or $\Gamma_0(q)$ then we call it a modular form of level q and a weight k. By using the functional equation we obtain

$$f(z) = f(z+1),$$

this tells us that f is a periodic function and therefore we can write a Fourier expansion for

f as

$$f(z) = \sum_{n=0}^{\infty} a(n) n^{(k-1)/2} e(nz). \tag{1.23}$$

If $a(0) = 0$ then we call *f* a cusp form. Using the Fourier coefficients $a(n)$ we form the *L*-function associated to *f*:

$$L(s,f) = \sum_{n=0}^{\infty} \frac{a(n)}{n^s}. \tag{1.24}$$

For many applications like bounding contour integrals and equidistribution problems it turns out that it is crucial to have estimates for the size of *L*-functions attached to modular/cusp forms inside the critical strip, and on the critical line. These *L*-functions satisfy functional equations, which implies an upper bound in the critical strip the so-called convexity bound,

$$L(s,f) \ll (k^2 |s^2| q)^{\frac{1}{4}+\varepsilon}.$$

It turns out that for many applications it suffices to replace the exponent $1/4$ by any smaller number. Such an estimate is called a subconvex bound. A method invented by Duke, Friedlander and Iwaniec has been used frequently in such problems. Their idea was to average over a family of *L*-functions, t hen by using an amplifier highlight the contribution of the *L*-functions under consideration. One of the main ingredients of their work was an estimation of a smooth version of

$$\sum_{\substack{am-bn=h \\ m,n<X}} d(m)d(n), \tag{1.25}$$

where $d(n)$ is the divisor function. They estimated (1.25) with an error term of order $O((abX)^{3/4})$. Note that we can consider sums of the type (1.25) with replacing $d(n)$ with Fourier coefficients of modular/cusp form. This is known as shifted convolution sums problem and it has many important applications such as proving the quantum unique ergodicity conjecture for Hecke-Maass forms on $SL_2(\mathbb{Z})\backslash\mathbb{H}$, a holomorphic analog of the quantum unique ergodicity conjecture and equidistribution of Heegner points.

In the last part of this thesis we improve this error term in the case $b = 1$. We also consider similar sums with $a = b = 1$ and $d(n)$ replaced by some other arithmetic sequences. There are two main ingredients in our proof.

1- We use the Voronoi type estimation of the following sum

$$\sum_{n=1}^{\infty} d(n)e\left(\frac{nd}{q}\right). \tag{1.26}$$

The Voronoi type summation formulas extract a main term from the above sum and gives an error term involving Bessel functions and the multiplicative inverses of d in $\mathbb{Z}/q\mathbb{Z}$. This estimate will help us to bring the Kloosterman sums into the picture.

2- We use the Kuznetsov formula to average the Kloosterman sums

$$S(m,n;q) = \sum_{\substack{1 \leq x < q \\ (x,q)=1}} e\left(\frac{mx + n\bar{x}}{q}\right) \tag{1.27}$$

with respect the parameter q. The celebrated Weil bound implies that

$$S(m,n;q) \leq d(q)\sqrt{\gcd(m,n,q)}\sqrt{q},$$

however on average over q it is expected that

$$S(m,n;q) \ll q^{\varepsilon}.$$

Kuznetsov's formula proves this for the smooth averaging over q and improves significantly what one obtains by Weil's bound for non-smooth averaging. By using these tools we proved the following

Theorem 1.10 (Aryan). *Let f be a smooth function supported on $[X, 2X] \times [X, 2X]$ satisfy-*

ing

$$\frac{\partial^{i+j}}{\partial x^i \partial y^j} f(x,y) \ll \frac{1}{X^{i+j}}. \tag{1.28}$$

For $h \ll X^{1-\varepsilon}$, We have

$$\sum_{am-n=h} d(m)d(n)f(am,n) = Main\ term(f,a,1) + O(X^{1/2+\theta+\varepsilon}), \tag{1.29}$$

where θ comes from the Ramanujan-Petersson conjecture and the current best bound is $\theta \leq 7/64$, due to Kim and Sarnak [49].

Note that the Main term has approximately order of magnitude X/a.
The above is one of the beautiful applications of modular forms in a problem that originated in classical analytic number theory.

Chapter 2

Distribution of squares modulo a composite number

2.1 Introduction

In this chapter we are mainly concerned with the distribution of subsets of integers that are not additively structured, though we will also prove results for sets that are additively structured. We begin by studying squares, which is the model example of a non-additively structured set. We continue with more complicated non-additively structured sets. The final part will be the study of the higher central moments of s-tuples of reduced residues. The content of this chapter appeared in *International Mathematics Research Notices* [4].

The distribution of squares modulo q

For q square-free, we call an integer s a square modulo q when s is a square modulo p for all primes p dividing q. Note that we count 0 as a square. Several authors have studied the distribution of spacings between squares modulo q. For q prime, a theorem of Davenport [15] shows that the probability of two consecutive squares modulo q being spaced h units apart is asymptotically 2^{-h} as q tends to infinity. For q square-free, Kurlberg and Rudnick [53] have shown that the distribution of spacings between squares approaches a Poisson distribution as $\omega(q)$ tends to infinity, where $\omega(q)$ is the number of distinct prime divisors of q.

Theorem 2.1 (Kurlberg and Rudnick)**.** *Let $\square$ be the symbol that denotes the word square*

and

$$\bar{s} = \frac{q}{\#\{x : x \text{ is } \square \text{ modulo } q\}},$$

and let I be an interval in $\mathbb{R}$ *that does not contain zero. Then*

$$\frac{\#\{(x_1, x_2) : x_1 - x_2 \in \bar{s}I : x_1, x_2 \text{ are } \square \bmod q\}}{\#\{x : x \text{ is a } \square \text{ modulo } q\}} = |I| + O\left(\frac{1}{s^{1-\varepsilon}}\right). \qquad (2.1)$$

Note that $\bar{s}$ is the mean spacing in the set of squares modulo q and the "probability" of a random integer being a square modulo q is $1/\bar{s}$, which approximately is $1/2^{\omega(q)}$. The results we prove in this chapter are, more or less, in the spirit of papers written by Montgomery and Vaughan [60] and Hooley [40, 41, 42]. These articles answer Erdős' question in [23] regarding the gaps between consecutive reduced residues. The reduced residues modulo q are the integers a_i, $1 = a_1 < a_2 < \ldots < a_{\phi(q)} < q$, that are relatively prime to q. Erdős [23] proposed the following conjecture for the second moment of the gap between consecutive reduced residues: For $\lambda = 2$ we have

$$V_\lambda(q) = \sum_{i=1}^{\phi(q)} (a_{i+1} - a_i)^\lambda \ll qP^{1-\lambda}, \qquad (2.2)$$

where $P = \phi(q)/q$ is the "probability" that a randomly chosen integer is relatively prime to q. Hooley [40] showed that (2.2) holds for all $0 < \lambda < 2$. For $\lambda = 2$, Hausman and Shapiro [33] gave a weaker bound than (2.2). Finally, Montgomery and Vaughan [60] succeeded in proving the conjecture, showing that (2.2) holds for all $\lambda > 0$. The key ingredient in the proof of the results of [40] and [33] is the variance of the random variable

$$\mathcal{R}_h(n) = \#\{m \in [n, n+h] : m \text{ is a reduced residue modulo } q\}.$$

In [60] variance and also higher central moments of $\mathcal{R}_h$ were studied. Motivated by the above results, we consider the variance of the following random variable. Let n be an

integer chosen uniformly at random in $\{1, 2, \ldots, q\}$, and define X_h by

$$X_h(n) = \#\{s \in [n, n+h] : s \text{ is a } \square \text{ modulo } q\}.$$

Theorem 2.2. *Let q be a square-free number and $P = \phi(q)/q$. Then as an upper bound we have*

$$\frac{1}{q}\sum_{n=0}^{q-1}\left(\sum_{\substack{m=1 \\ n+m \text{ is } \square \bmod q}}^{h} 1 - \frac{h}{2^{\omega(q)}P}\right)^2 \le \frac{h}{2^{\omega(q)}P}\prod_{p|q}\left(1+\frac{1}{\sqrt{p}}\right), \tag{2.3}$$

and as a lower bound we have

$$\frac{h}{4^{\omega(q)}P}\sum_{\substack{r>h^2 \\ r|q}}\prod_{p|r}\left(1-\frac{3}{\sqrt{p}}\right) \ll \frac{1}{q}\sum_{n=0}^{q-1}\left(\sum_{\substack{m=1 \\ n+m \text{ is } \square \bmod q}}^{h} 1 - \frac{h}{2^{\omega(q)}P}\right)^2. \tag{2.4}$$

Moreover, if the prime divisors of q are all congruent to 3 modulo 4 then we have the sharper bound

$$\frac{1}{q}\sum_{n=0}^{q-1}\left(\sum_{\substack{m=1 \\ n+m \text{ is } \square \bmod q}}^{h} 1 - \frac{h}{2^{\omega(q)}P}\right)^2 \le \frac{h}{2^{\omega(q)}P^2}. \tag{2.5}$$

Remark 2.3. Note that in (2.3), $\prod_{p|q}(1 + p^{-1/2}) \ll 2^{\sqrt{\omega(q)}}$ which is much smaller than $2^{\omega(q)}$ for large $\omega(q)$. For the mean of X_h, we have $\mathbf{E}(X_h) = \frac{h}{2^{\omega(q)}P}$ and therefore the left hand side of (2.3) is equal to the variance of X_h, which we denote by $\mathbf{Var}(X_h)$. Consequently, Theorem 2.2 implies the following upper bound:

$$\mathbf{Var}(X_h) \le \prod_{p|q}\left(1+\frac{1}{\sqrt{p}}\right)\cdot \mathbf{E}(X_h),$$

whereas the trivial upper bound is

$$\mathbf{Var}(X_h) \le \mathbf{E}(X_h)^2.$$

Remark 2.4. Theorem 2.12 yields non trivial bound when $h \ge 2^{\omega(q)}P$. This is the case that

17

there is a possibility of cancellation in

$$\sum_{\substack{m=1 \\ n+m \text{ is } \square \bmod q}}^{h} 1 - \frac{h}{2^{\omega(q)}P}.$$

Remark 2.5. Let N be the set of quadratic non-residues modulo a prime p. The reason for the better bound (2.5) is that, when $p \equiv 3 \bmod 4$, the size of the Fourier coefficient $\sum_{n \in N} e(n/p)$ of N, is smaller than when $p \equiv 1 \bmod 4$.

In 1936 Cramer [14], assuming the Riemann hypothesis (RH), showed the following result concerning the average gap between consecutive primes:

$$\sum_{p_n < x} (p_{n+1} - p_n)^2 \ll x(\log x)^{3+\varepsilon}. \tag{2.6}$$

This bound was the inspiration of Erdős' conjecture (2.2). Using Theorem 2.2, we prove an analogous result for gaps between squares.

Corollary 2.6. *Let s_i be the squares modulo q in increasing order. Then*

$$\frac{1}{q} \sum_{s_i < q} (s_{i+1} - s_i)^2 \ll 2^{\omega(q)} P(\log q) \prod_{p|q} \left(1 + \frac{1}{\sqrt{p}}\right). \tag{2.7}$$

Remark 2.7. It seems plausible that the factor $\prod_{p|q}(1 + p^{-1/2})$ can be removed from the right hand side of (2.7). Also, it seems difficult to estimate the higher moments in Corollary 0.1. Indeed, in the simple case where q equals a prime number p, a good estimation of the higher moments would imply that the gap between two consecutive quadratic residues is less than $p^{o(1)}$. Note that the best known bound obtained by Burgess [9] is $p^{1/4+o(1)}$.

An important property of the squares that we use in the proof of Theorem 2.2 is the following: For $a \neq 0$ modulo p we have

$$\left| \sum_{s \text{ is } \square \bmod p} e\left(\frac{sa}{p}\right) \right| \ll \sqrt{p}. \tag{2.8}$$

18

In the language of Fourier Analysis, this property means that all of the non-trivial Fourier coefficients of the set of squares have square root cancellation. In the context of this chapter we denote the property of having small Fourier coefficient as being "non-additively structured". In the next section we generalize Theorem 2.2 for all the sets that are not additively structured. We also use similar ideas to study a problem related to additive combinatorics which is known as the inverse conjecture for the large sieve.

Relation with the inverse conjecture for the large sieve

In this section we consider the inverse conjecture for the large sieve. We also introduce the notions of "additively structured" and "non-additively structured" sets and study the distribution of these sets. Based on these ideas we formulate a refined version of the inverse conjecture. Roughly speaking, we say that a subset of $\mathbb{Z}/p\mathbb{Z}$ is not additively structured if all of its non-trivial Fourier coefficients have square root cancellation. On the other hand, being additively structured means there exist at least one large Fourier coefficient. Having a large Fourier coefficient is equivalent to saying that the set has many quadruples (x_1, x_2, x_3, x_4) such that $x_1 + x_2 = x_3 + x_4$, which explains the reason for choosing the "additive structure" terminology.

Let A be a finite set of integers with the property that the reduced set A (mod p) occupies at most $(p+1)/2$ residue classes modulo p for every prime $p|q$. In other words, for $p|q$ and $\Omega_p \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|\Omega_p| = (p-1)/2$, A is obtained by sieving $[1, X]$ by all the congruence classes in Ω_p. The inverse problem for the large sieve is concerned with the size of A (see [38]). In the case where q is equal to the product of all primes less than $\sqrt{X}$, using the large sieve inequality one can show that $|A| \ll \sqrt{X}$. The following is the formulation of the conjecture by Green [30].

Conjecture 2.8 (**Inverse conjecture for the large sieve**)**.** For every prime number $p < \sqrt{X}$, let $\Omega_p \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|\Omega_p| = (p-1)/2$. Let $A \subseteq \{1, 2, \ldots, X\}$ be the set obtained by sieving

out the residue classes in Ω_p for $p < X$. Then $|A| \ll X^\varepsilon$ unless A is contained in the set of values of a quadratic polynomial $f(n) = an^2 + bn + c$, with the possible exception of a set of size X^ε.

Remark 2.9. This has been stated informally in the literature as follows. If the size of A is not too small then A should possesses an "algebraic" structure. The problem with this statement is that a formal definition for possessing an "algebraic" structure has not been given. Although it seems that any set with "algebraic" structure is not additively structured, the reverse may not be true.

Here our aim is to look at this problem from the distributional aspect. We consider A to be a subset of an interval larger than the interval $[1, X]$. We fix A to be a subset of $\{1, 2, \ldots, q\}$. This set shall be defined by sieving out congruence classes in Ω_p for all $p | q$, $|\Omega_p| = (p-1)/2$. Next we let n be an integer picked uniformly at random in $\{1, 2, \ldots, q\}$, and define the random variable $\mathcal{Y}_h$ by

$$\mathcal{Y}_h(n) = |[n, n+h] \cap A|. \tag{2.9}$$

Since $|\Omega_p| = (p-1)/2$, the Chinese Remainder Theorem implies that

$$|A| = \prod_{p|q} \left(\frac{p+1}{2} \right).$$

Question: How is A distributed modulo q?

We will prove a result which shows that if for all $p | q$, Ω_p is not additively structured, then A is well distributed. In the other direction we show some partial results in the case that Ω_p is additively structured. The latter result indicates that A is far from being well distributed. To make the notion of being well distributed more clear in the context of this chapter, let $A \subseteq [1, q]$ and define $\mathrm{Prob}(x \in A) = |A|/q$. We say that A is well distributed if any interval of length h inside $[1, q]$, contains $h \frac{|A|}{q}(1 + o(1))$ elements of A.

20

Now we introduce the notion of a set that is "not additively structured". We describe this using the example of squares. In this case Ω_p is the set of non-quadratic residues modulo p. In other words in order to end up with squares after sieving, we need to sieve out integers congruent to non-quadratic residues modulo each prime $p|q$. Inspired by the property of squares mentioned in the Equation (2.8), we have the following definition.

Definition 2.10 (**Not additively structured**). For p a prime number we say that $\Omega_p \subseteq \mathbb{Z}/p\mathbb{Z}$ is not additively structured if for all $a \neq 0$ modulo p,

$$\left| \sum_{x \in \Omega_p} e\left(\frac{ax}{p}\right) \right| < c_p \sqrt{p}, \tag{2.10}$$

where c_p depends on p and satisfies $c_p \ll \log p$.

We will give two examples of sets that are not additively structured.

Example 1. By using the following theorem of Weil we can show that the image of a polynomial P is not additively structured under the following condition: For every $y \in \text{Im}(P)$ the equation $P(x) = y \ (\text{mod } p)$ has the same number of solutions, with the exception of a subset $\mathcal{E}$ of the image with $|\mathcal{E}| \ll \sqrt{p}$.

Theorem 2.11 (Weil). *Let $P \in \mathbb{Z}[X]$ be a polynomial of degree $d > 1$. Let p be a prime such that $\gcd(d, p) = 1$. Then we have*

$$\left| \sum_{x \, (\text{mod } p)} e\left(\frac{P(x)}{p}\right) \right| < (d-1)\sqrt{p}. \tag{2.11}$$

Example 2. Another example of a set that is not additively structured is

$$\Omega_{K,p} := \{x + y : 1 \leq x, y \leq p - 1 \text{ and } xy \equiv 1 \text{ mod } p\}. \tag{2.12}$$

This can be shown by using the Weil bound [68] on Kloosterman sums. The size of $\Omega_{K,p}$ is

$(p+1)/2$. One open problem regarding this asks about existence of small residue classes with small reciprocal. More precisely let

$$M_p := \min_{x \not\equiv 0 \bmod p} \left\{ \max\{x, x^{-1}\} \right\}. \tag{2.13}$$

Then the question is how small can M_p be? As an application of the Weil bound on Kloosterman sums one can show that $M_p \leq 2(\log p)p^{3/4}$ (see [37]). It seems natural to conjecture that $M_p \leq p^{1/2+\varepsilon}$. In fact Tao [65] even suggested that $M_p = O(p^{1/2})$ might be possible. Using Theorem 2.12 one can show that there exist x modulo p such that

$$x + x^{-1} \bmod p \leq p^{1/2+\varepsilon}. \tag{2.14}$$

For such x if $x +_{\mathbb{Z}} x^{-1} < p$, then (2.14) would imply the conjectural bound for M_p. However if $x +_{\mathbb{Z}} x^{-1} \geq p$, then (2.14) does not give any useful information. Thus it would be interesting to look at the distribution of the set

$$\Omega'_{K,p} := \left\{ x + x^{-1} : 1 \leq x, x^{-1} \leq p-1 \text{ and } x +_{\mathbb{Z}} x^{-1} < p \right\}. \tag{2.15}$$

If $\Omega'_{K,p}$ were not additively structured then it would imply the conjectural bound for M_p. However in Theorem 2.20, we will show that this is not the case and $\Omega'_{K,p}$ is not well distributed modulo p. Consequently one way to attack the conjectural bound on M_p would be to find a proper subset of $\Omega'_{K,p}$ which is not additively structured. Another way would be to add certain elements to $\Omega'_{K,p}$ in order to make a set that is not additively structured.

We show that if Ω_p is not additively structured then A is well distributed.

Theorem 2.12. *Let $\mathcal{Y}_h$ be as (2.9). Then if Ω_p is not additively structured i.e., satisfies*

22

(2.10) and $|\Omega_p| = (p-1)/2$, then we have

$$\frac{1}{q}\sum_{n=0}^{q-1}\left(\sum_{\substack{m\in[n,n+h]\\ m\notin\Omega_p \bmod p\\ \forall p|q}}1 - h\prod_{p|q}\left(\frac{p+1}{2p}\right)\right)^2 \ll h\prod_{p|q}\left(\left(\frac{p+1}{2p}\right)^2 + c_p^2\right), \qquad (2.16)$$

or equivalently

$$\mathbf{Var}(\mathcal{Y}_h) \ll \mathbf{E}(\mathcal{Y}_h)\prod_{p|q}\left(\frac{p+1}{2p} + \frac{2c_p^2 p}{p+1}\right), \qquad (2.17)$$

where c_p is the constant in (2.10).

Remark 2.13. Note that c_p can never be too small. In fact one can get a lower bound $c_p > 1/2$. As a result the right hand side of (2.16) is always bigger than $h/2^{\omega(q)}$.

Remark 2.14. Note that the trivial upper bound on $\mathbf{Var}(\mathcal{Y}_h)$ is $\mathbf{E}(\mathcal{Y}_h)^2$. In section 3 we prove a more general result without the restriction $|\Omega_p| = (p-1)/2$ (see Lemma 2.24).

Remark 2.15. By taking Ω_p equal to the set of quadratic non-residues in Theorem 2.12, we obtain Theorem 2.2.

Returning to the inverse conjecture for the large sieve, Green and Harper [31] proved the conjecture when Ω_p is an interval and gave a non-trivial result when Ω_p has certain additive structure. This brings us to the definition of a set with additive structure.

Definition 2.16 (**Additively structured**). For p a prime number we say that $\Omega_p \subseteq \mathbb{Z}/p\mathbb{Z}$ is additively structured if there exist $a \neq 0$ modulo p,

$$\left|\sum_{x\in\Omega_p}e\left(\frac{ax}{p}\right)\right| \geq C_p p, \qquad (2.18)$$

where C_p depends on p and here we consider $C_p \gg \log^{-1} p$.

Remark 2.17. Note that additively structured is the extreme opposite of not additively structured, since the opposite of not additively structured means every set has a Fourier coeffi-

cient just bigger than $p^{1/2+\varepsilon}$, while being additively structured means there exists a Fourier coefficient bigger than $p^{1-\varepsilon}$.

Let $\Omega_p = \{0, 2, 4, \ldots, p-1\}$, for all $p|q$. Note that this set is additively structured since for $a = (p+1)/2$ we have

$$\left| \sum_{x \in \Omega_p} e\left(\frac{xa}{p}\right) \right| = \left| \frac{e\left(\frac{1}{2p}\right) + 1}{e\left(\frac{1}{p}\right) - 1} \right| \geq \frac{p}{\pi}.$$

For the set A we prove a result which shows that A is far from being well distributed.

Theorem 2.18. *Let* $\Omega_p = \{0, 2, 4, \ldots, p-1\}$ *and* $\mathcal{Y}_h$ *be as* (2.9). *Assume* $q = p_1, \ldots, p_{\lfloor \log X \rfloor}$, *where* $X < p_i < 2X$ *and* $|p_2 - p_1| \ll \log p_1$. *Then for every integer* $h < \frac{X^2}{\log X}$ *we have that*

$$\frac{1}{q} \sum_{n=0}^{q-1} \left(\sum_{\substack{m \in [n, n+h] \\ m \notin \Omega_p \bmod p \\ \forall p | q}} 1 - h \prod_{p | q} \left(\frac{p+1}{2p} \right) \right)^2 \gg \left(\frac{h}{2^{\omega(q)} P} \right)^2,$$

or equivalently

$$\mathbf{Var}(\mathcal{Y}_h) \gg \mathbf{E}(\mathcal{Y}_h)^2.$$

Theorem 2.12 shows a connection between non-additive structure in sets Ω_p and well distribution of A. Theorems 2.18 shows a connection between the additive structure of the sets Ω_p and A not being well distributed. Recall that A is obtained by sieving out the congruence classes in Ω_p. In the inverse conjecture for the large sieve, there is a similar connection between the size of the sifted set and the additive structure of Ω_p. More precisely, if the size of the sifted set A is not too small, then A is the image of a quadratic polynomial and from Example 1 we know that the image of a quadratic polynomial is not additively structured. Thus if the size of A is large then A is not additively structured. Inspired by this observation it seems natural to refine the inverse conjecture for the large sieve in terms of the additive

structure of A. Now we state our conjecture.

Conjecture 2.19. Let A be the subset of $[1, X]$ obtained by sieving out congruence classes in Ω_p for $p < X^{1/2}$. Moreover assume that for each p, Ω_p is additively structured i.e. Ω_p has the property that there exist $a \neq 0$ modulo p such that

$$\left| \sum_{x \in \Omega_p} e\left(\frac{ax}{p}\right) \right| \gg C_p p,$$

with $C_p \gg \log^{-1} p$. Then

$$|A| \ll X^{\varepsilon}.$$

Harper and Green [31] proved a non-trivial bound for the size of A in the above conjecture. They proved that if Ω_p has many quadruples (x_1, x_2, x_3, x_4) such that $x_1 + x_2 = x_3 + x_4$, then there exists $c > 0$ such that $|A| \ll X^{1/2 - c}$. Note that the quadruple condition is equivalent to Ω_p having a large Fourier coefficient. (Larger than $p^{1-\varepsilon}$.)

To finish this part of the article we state a result regarding the distribution of $\Omega'_{K,p}$ from Example 2. Note that

$$|\Omega'_{K,p}| = \begin{cases} \frac{p+1}{4} & \text{if } p \equiv 3 \bmod 4, \\[2mm] \frac{p-1}{4} & \text{if } p \equiv 1 \bmod 4. \end{cases} \tag{2.19}$$

Theorem 2.20. *Let* $\Omega'_{K,p}$ *be as in* (2.15). *Then for* $h < p/2$ *we have*

$$\frac{1}{p} \sum_{n=0}^{p-1} \left(\sum_{\substack{m \in [n, n+h] \\ m \in \Omega'_{K,p}}} 1 - \frac{h}{p} |\Omega'_{K,p}| \right)^2 \gg h^2. \tag{2.20}$$

In the last part of this article we study the distribution of s-tuples of reduced residues. Although the following theorem is independent than previous results, the techniques are very

similar. In particular Lemma 2.23 will be applied in all theorems.

Higher central moments for the distribution of *s*-tuples of reduced residues

Let

$$\mathcal{D} = \{h_1, h_2, \ldots, h_s\},$$

and $\nu_p(\mathcal{D})$ be the number of distinct elements in $\mathcal{D}$ mod p. We call $\mathcal{D}$ *admissible* if $\nu_p(\mathcal{D}) < p$ for all primes p. We call $(a + h_1, \ldots, a + h_s)$ an *s-tuple of reduced residues* if each element $a + h_i$ is coprime to q. In our previous results we were only able to calculate the variance and could not obtain any estimate for higher moments. The reason for this, in a sieve-theoretic language, is that when $|\Omega_p| = (p-1)/2$, as q tends to infinity the dimension of the sieve also tends to infinity. However, if we fix our admissible set and look at the distribution of *s*-tuples of reduced residues, then the dimension stays bounded and consequently we are able to derive results for higher moments. Let $k_q(m)$ be the characteristic function of reduced residues, that is to say

$$k_q(m) = \begin{cases} 1 & \text{if } \gcd(m, q) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

The generalization of Erdős' conjecture, i.e.

$$V_2^{\mathcal{D}}(q) = \sum_{\substack{(a_i + h_j, q) = 1 \\ h_j \in \mathcal{D}}} (a_{i+1} - a_i)^2 \ll q P^{-s}, \tag{2.21}$$

concerns the gap between *s*-tuples of reduced residues. In order to prove the generalization of Erdős' conjecture (see [23] and [3]), the author in [3] studied the *k*-th moment of the

distribution of the *s*-tuples of reduced residues: Let

$$M_k^{\mathcal{D}}(q,h) := \sum_{n=0}^{q-1}\left(\sum_{m=1}^{h} k_q(n+m+h_1)\dots k_q(n+m+h_s) - h\prod_{p|q}\left(1 - \frac{\nu_p(D)}{p}\right)\right)^k.$$

In the case $s=1$, i.e. $\mathcal{D}=\{0\}$, and $k<2$ this was studied by Hooley [40] who found an upper bound for $M_2^{\{0\}}(q,h)$. Hausman and Shapiro [33] gave an exact formula for $M_2^{\{0\}}(q,h)$. Their formula immediately gives the upper bound $M_2^{\{0\}}(q,h) \leq qhP$. Finally, for a fixed natural number k, Montgomery and Vaughan [60] showed

$$M_k^{\{0\}}(q,h) \leq q(hP)^{k/2} + qhP. \tag{2.22}$$

For a fixed admissible set $\mathcal{D}$ it was proven in [3] that

$$M_k^{\mathcal{D}}(q,h) \ll_{s,k} qh^{k/2}P^{-2ks+ks}. \tag{2.23}$$

This was enough to get the generalization of Erdős' conjecture, however the method failed to get bounds as strong as (2.22). In the last section of this chapter we improve (2.23).

Theorem 2.21. *Let* $P = \phi(q)/q$. *For* $h < \exp\left(\frac{1}{kP^{1/s}}\right)$, *we have*

$$M_k^{\mathcal{D}}(q,h) \ll_{s,k} q(hP^s)^{k/2} \tag{2.24}$$

and in general

$$M_k^{\mathcal{D}}(q,h) \ll_{s,k} qh^{k/2}P^{sk-s^2\frac{k}{2}}. \tag{2.25}$$

Remark 2.22. Note that (2.24) is the best possible upper bound and it matches the upper bound derived from probabilistic estimates (see [3, Lemma 2.1]).

The open question that remains here is whether or not the bound (2.25) is sharp. In other

words, is there an admissible set $\mathcal{D}$ such that for $h \geq \exp\left(\frac{1}{kP^{1/s}}\right)$, we have

$$M_k^{\mathcal{D}}(q,h) \gg_{s,k} qh^{k/2}P^{sk-s^2\frac{k}{2}}?$$

Notation

Throughout the chapter we use the symbol $\square$ as an abbreviation for the word "square". For example, "a is a $\square$ modulo q" reads "a is a square modulo q". Also, for functions $g(x)$ and $h(x)$, we use interchangeably Landau's and Vinogradov's notation $g(x) = O(h(x))$, $g(x) \ll h(x)$ or $h(x) \gg g(x)$ to indicate that there exists a constant $C > 0$ such that $|g(x)| \leq C|h(x)|$ for all x. We use subscripts such as $\ll_{s,k}$ to indicate that the constant C may depend on parameters s,k. We let ϕ denote the Euler's totient function, defined by $\phi(q) = \#\{1 \leq n \leq q : (n,q) = 1\}$. We also write $P = \phi(q)/q$ and we let $+_{\mathbb{Z}}$ denote the addition in $\mathbb{Z}$, as opposed to modular addition.

2.2 Main estimate

In this section we prove an exponential identity for the indicator function of s-tuples of reduced residues.

Lemma 2.23. *Let $\mathcal{D} = \{h_1, \ldots, h_s\}$ be an admissible set. For square-free integers q we have*

$$k_q(m+h_1)\ldots k_q(m+h_s) = P_{\mathcal{D}} \sum_{r|q} \frac{\mu(r)}{\phi_{\mathcal{D}}(r)} \sum_{\substack{a<r \\ (a,r)=1}} e\left(m\frac{a}{r}\right)\mu_{\mathcal{D}}(a,r),$$

where

$$\mu_{\mathcal{D}}(a,r) = \prod_{p|r}\left(\sum_{s\in\mathcal{D}_p} e\left(\frac{sa(r/p)_p^{-1}}{p}\right)\right),$$

$$\phi_{\mathcal{D}}(r) = \prod_{p|r}(p - \nu_p(\mathcal{D})),$$

$$P_{\mathcal{D}} = \frac{\prod_{p|q}(p - \nu_p(\mathcal{D}))}{q},$$

$(r/p)_p^{-1}$ is the inverse of r/p in $(\mathbb{Z}/p\mathbb{Z})^*$, and $\mathcal{D}_p$ consists of the reduction of elements of

28

$\mathcal{D}$ modulo p.

Proof. The starting point in the method of Montgomery and Vaughan [60] is to use the following Fourier expansion of the indicator function of reduced residues:

$$k_q(m) = \sum_{r|q} \frac{\mu(r)}{r} \sum_{0 \le b < r} e\left(m\frac{b}{r}\right).$$

Using this expansion, we deduce that

$$
\begin{aligned}
k_q(m+h_1)&\dots k_q(m+h_s) \\
&= \sum_{r_1,r_2,\dots,r_s|q} \frac{\mu(r_1)\dots\mu(r_s)}{r_1\dots r_s} \sum_{\substack{0<a_i\le r_i \\ \sum_{i=1}^s \frac{a_i}{r_i}=\frac{a}{r}}} e\left(\sum_{i=1}^s (m+h_i)\frac{a_i}{r_i}\right) \\
&= \sum_{\substack{r|q \\ a\le r \\ (a,r)=1}} e\left(m\frac{a}{r}\right) \sum_{r_1,r_2,\dots,r_s|q} \frac{\mu(r_1)\dots\mu(r_s)}{r_1\dots r_s} \sum_{\substack{0<a_i\le r_i \\ \sum_{i=1}^s \frac{a_i}{r_i}=\frac{a}{r}}} e\left(\sum_{i=1}^s h_i\frac{a_i}{r_i}\right).
\end{aligned}
$$

We fix a, r and therefore it is enough to show that

$$
\sum_{r_1,r_2,\dots,r_s|q} \frac{\mu(r_1)\dots\mu(r_s)}{r_1\dots r_s} \sum_{\substack{0<a_i\le r_i \\ \sum_{i=1}^s \frac{a_i}{r_i}=\frac{a}{r}}} e\left(\sum_{i=1}^s h_i\frac{a_i}{r_i}\right) \tag{2.26}
$$

$$
= P_{\mathcal{D}} \frac{\mu(r)}{\phi_{\mathcal{D}}(r)} \prod_{p|r}\left(\sum_{s\in\mathcal{D}_p} e\left(\frac{sa(r/p)_p^{-1}}{p}\right)\right).
$$

To show this, note that we can write

$$\frac{a}{r} \equiv \sum_{p|q} \frac{a_p}{p} \pmod{1}$$

uniquely where $0 \le a_p < p$. Fixing $p_0|r$, we have that

$$\frac{a}{r} \cdot \frac{r}{p_0} \equiv \frac{a}{p_0} \equiv \frac{a_{p_0}}{p_0}\left(\frac{r}{p_0}\right) \pmod{1}, \tag{2.27}$$

hence $a \equiv a_{p_0}\left(\dfrac{r}{p_0}\right)$ (mod p_0). Since q, and consequently r, are square-free, $\left(\frac{r}{p_0}, p_0\right) = 1$, so for $a_{p_0} \neq 0$, we have that $a_{p_0} \equiv a\left(\dfrac{r}{p_0}\right)^{-1}_{p_0}$ (mod p_0). Using (2.27), we can can write the left hand side of the (2.26) in terms of the prime divisors of q. Therefore (2.26) is equal to

$$\prod_{p|q} \sum_{q_i|p} \frac{\mu(q_1)\dots\mu(q_s)}{q_1\dots q_s} \sum_{\substack{0 \leq a_i < q_i \\ \sum \frac{a_i}{q_i} = \frac{a_p}{p}}} e\left(\sum_{i=1}^{s} h_i \frac{a_i}{q_i}\right).$$

To simplify the condition $\sum \frac{a_i}{q_i} = \frac{a_p}{p}$, we write

$$\sum_{\substack{0 \leq a_i < q_i \\ \sum \frac{a_i}{q_i} = \frac{a_p}{p}}} e\left(\sum_{i=1}^{s} h_i \frac{a_i}{q_i}\right) = \sum_{v=1}^{p} \frac{1}{p} \sum_{0 \leq a_i < q_i} e\left(\left(\frac{a_p}{p} - \sum_{i=1}^{s} \frac{a_i}{q_i}\right)v\right) e\left(\sum_{i=1}^{s} h_i \frac{a_i}{q_i}\right).$$

Therefore (2.26) is equal to

$$\prod_{p|q} \sum_{q_i|p} \frac{\mu(q_1)\dots\mu(q_s)}{q_1\dots q_s} \sum_{v=1}^{p} \frac{1}{p} \sum_{0 \leq a_i < q_i} e\left(\left(\frac{a_p}{p} - \sum_{i=1}^{s} \frac{a_i}{q_i}\right)v\right) e\left(\sum_{i=1}^{s} h_i \frac{a_i}{q_i}\right)$$

$$= \prod_{p|q} \sum_{v=1}^{p} \frac{e\left(v\frac{a_p}{p}\right)}{p} \prod_{i=1}^{s} \sum_{q_i|p} \frac{\mu(q_i)}{q_i} \sum_{0 \leq a_i < q_i} e\left(\frac{a_i}{q_i}(h_i - v)\right)$$

$$= \prod_{p|q} \sum_{v=1}^{p} \frac{e\left(v\frac{a_p}{p}\right)}{p} \prod_{i=1}^{s} \left(1 - \frac{1}{p} \sum_{a \leq p} e\left(\frac{a}{p}(h_i - v)\right)\right)$$

$$= \prod_{p|q} \sum_{\substack{v=1 \\ v \neq h_i \bmod p \\ h_i \in \mathcal{D}}}^{p} \frac{e\left(v\frac{a_p}{p}\right)}{p} = \frac{\phi_{\mathcal{D}}(q)r}{q\phi_{\mathcal{D}}(r)} \prod_{p|r} \frac{\mu(p)}{p} \sum_{\substack{s \equiv h_i \bmod p \\ h_i \in \mathcal{D} \\ a_p \neq 0}} e\left(s\frac{a_p}{p}\right).$$

The last equality holds since $a_p = 0$ for $p \nmid r$, and for $a_p \neq 0$ we have that

$$\sum_{\substack{v=1 \\ v \neq h_i \bmod p \\ h_i \in \mathcal{D}}}^{p} e\left(v\frac{a_p}{p}\right) = -\sum_{s \in \mathcal{D}_p} e\left(s\frac{a_p}{p}\right).$$

This completes the proof of the lemma. $\qquad\qquad\square$

2.3 Distribution of squares modulo q

In this section we are going to prove Theorem 2.12 and Corollary 2.6. Before proceeding with the proof we derive a formula for the left hand side of (2.3). For q square-free, x is a square modulo q if and only if x is a square modulo p for all primes p dividing q. For each p which divides q, let $\mathcal{D}_p := \{h_{1,p}, \ldots, h_{\nu_p, p}\}$. By the Chinese Reminder Theorem there exists a set $\mathcal{D} = \{h_1, \ldots, h_s\}$, such that $\mathcal{D}$ modulo p is equal to $\mathcal{D}_p$, for all $p|q$. For instance let $h_1, h_2, \ldots h_s$ to be uniquely selected to satisfy the following congruences $h_i \equiv h_{i,p}$ mod p, for all $p|q$. In the case that $i > \nu_p$ and therefore $h_{i,p}$ does not exist, we take $h_{i,p}$ to be equal $h_{\nu_p, p}$. This explains how we can construct the set $\mathcal{D}$.

Now if

$$k_q(m+h_1) \ldots k_q(m+h_s) = 1,$$

then $m \not\equiv -h_{i,p}$ modulo p, for $1 \leq i \leq \nu_p$ and for all p dividing q. We now let

$$\mathcal{D}_p = \{-n_1, \ldots, -n_{\frac{p-1}{2}}\}, \tag{2.28}$$

where n_i's are quadratic non-residues modulo p. From $k_q(m+h_1) \ldots k_q(m+h_s) = 1$, it follows that m is a square modulo q. Using Lemma 2.23 we have that

$$k_q(m+h_1) \ldots k_q(m+h_s) = \prod_{p|q} \frac{\frac{p+1}{2}}{p} \sum_{r|q} \frac{\mu(r)}{\prod_{p|r} \frac{p+1}{2}} \sum_{\substack{a \leq r \\ (a,r)=1}} e\left(m\frac{a}{r}\right) \mu_{\mathcal{D}}(a,r)$$

$$= \frac{1}{2^{\omega(q)} P} \sum_{r|q} \frac{\mu(r)}{\prod_{p|r} \frac{p+1}{2}} \sum_{\substack{a \leq r \\ (a,r)=1}} e\left(m\frac{a}{r}\right) \mu_{\mathcal{D}}(a,r), \tag{2.29}$$

where $P = \frac{\phi(q)}{q}$. Summing this from $m = n+1$ to $n+h$ and then subtracting the term corresponding to $r = 1$ we have

$$
\sum_{m=n+1}^{n+h} k_q(m+h_1)\ldots k_q(m+h_s) - \frac{h}{2^{\omega(q)}P}
$$
$$
= \frac{1}{2^{\omega(q)}P} \sum_{\substack{r|q \\ r>1}} \frac{\mu(r)}{\prod_{p|r} \frac{p+1}{2}} \sum_{\substack{a<r \\ (a,r)=1}} E\left(\frac{a}{r}\right)\mu_{\mathcal{D}}(a,r)e\left(n\frac{a}{r}\right), \tag{2.30}
$$

where

$$
E(x) = \sum_{m=1}^{h} e(mx).
$$

We square (2.30) and sum from $n = 1$ to q to obtain

$$
\sum_{n=0}^{q-1}\left(\sum_{m=1}^{h} k_q(n+m+h_1)\ldots k_q(n+m+h_s) - \frac{h}{2^{\omega(q)}P}\right)^2 = \tag{2.31}
$$
$$
\frac{q}{4^{\omega(q)}P^2} \sum_{\substack{r_1,\,r_2|q \\ r_1,r_2>1}} \frac{\mu(r_1)\mu(r_2)}{\prod_{p|r_1}\frac{p+1}{2}\prod_{p|r_2}\frac{p+1}{2}} \sum_{\substack{a_i<r \\ (a_i,r_i)=1 \\ i=1,2 \\ \frac{a_1}{r_1}+\frac{a_2}{r_2}\in\mathbb{Z}}} E\left(\frac{a_1}{r_1}\right)E\left(\frac{a_2}{r_2}\right)\mu_{\mathcal{D}}(a_1,r_1)\mu_{\mathcal{D}}(a_2,r_2).
$$

Now we are prepared to prove the Theorem 2.2.

Proof of Theorem 2.2. From the condition $\dfrac{a_1}{r_1} + \dfrac{a_2}{r_2} \in \mathbb{Z}$ in (2.31) it follows that $r_1 = r_2$ and $a_2 = r - a_1$, thus we have

$$
\sum_{n=0}^{q-1}\left(\sum_{\substack{m=1 \\ n+m \text{ is } \square \bmod q}}^{h} 1 - \frac{h}{2^{\omega(q)}P}\right)^2 = \frac{q}{4^{\omega(q)}P^2}\sum_{\substack{r|q \\ r>1}}\frac{4^{\omega(r)}}{\prod_{p|r}(p+1)^2}\sum_{\substack{a<r \\ (a,r)=1}}\left|E\left(\frac{a}{r}\right)\mu_{\mathcal{D}}(a,r)\right|^2.
$$

$$\tag{2.32}$$

Now, we need to bound $\mu_{\mathcal{D}}(a,r)$. For each n_i in $\mathcal{D}_p$ in (2.28), employing the Legendre symbol

$$
\left(\frac{-n_i a(r/p)^{-1}}{p}\right) = -\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)\left(\frac{(r/p)^{-1}}{p}\right).
$$

Since $a \neq 0$ the sequence $\left\{ -n_i a (r/p)^{-1} \right\}$ is either the sequence of quadratic residues or the sequence of quadratic non-residues modulo p. Using the Gauss bound for exponential sums over quadratic residues (respectively non-residues) [16, Page 13]

$$\left| \sum_i e\left(\frac{n_i a (r/p)_p^{-1}}{p} \right) \right| = \begin{cases} \frac{\sqrt{p}-1}{2} & \text{if } \left(\frac{-a(r/p)^{-1}}{p} \right) = -1, \\ \frac{\sqrt{p}+1}{2} & \text{otherwise,} \end{cases} \tag{2.33}$$

if $p \equiv 1$ modulo 4 and

$$\left| \sum_i e\left(\frac{n_i a (r/p)_p^{-1}}{p} \right) \right| = \frac{\sqrt{p}+1}{2} \tag{2.34}$$

if $p \equiv 3$ modulo 4. Consequently, for $a \neq 0$,

$$\prod_{p|r} \frac{\sqrt{p}-1}{2} \leq |\mu_{\mathcal{D}}(a,r)| \leq \prod_{p|r} \frac{\sqrt{p}+1}{2}. \tag{2.35}$$

Using this in (2.32) we have the upper bound

$$\sum_{n=0}^{q-1} \left(\sum_{\substack{m=1 \\ n+m \text{ is } \square \bmod q}}^{h} 1 - \frac{h}{2^{\omega(q)} P} \right)^2 \leq \frac{q}{4^{\omega(q)} P2} \sum_{\substack{r|q \\ r>1}} \prod_{p|r} \frac{\left(\sqrt{p}+1\right)^2}{(p+1)^2} \sum_{\substack{a<r \\ (a,r)=1}} \left| E\left(\frac{a}{r}\right) \right|^2, \tag{2.36}$$

and the lower bound

$$\frac{q}{4^{\omega(q)} P2} \sum_{\substack{r|q \\ r>1}} \prod_{p|r} \frac{\left(\sqrt{p}-1\right)^2}{(p+1)^2} \sum_{\substack{a<r \\ (a,r)=1}} \left| E\left(\frac{a}{r}\right) \right|^2 \leq \sum_{n=0}^{q-1} \left(\sum_{\substack{m=1 \\ n+m \text{ is } \square \bmod q}}^{h} 1 - \frac{h}{2^{\omega(q)} P} \right)^2. \tag{2.37}$$

Using the bound([60, Lemma 4]),

$$\sum_{\substack{a<r \\ (a,r)=1}} \left| E\left(\frac{a}{r}\right) \right|^2 < r \min(r,h), \tag{2.38}$$

and by employing this bound in (2.36) we have

$$\sum_{n=0}^{q-1}\left(\sum_{\substack{m=1\\ n+m \text{ is } \square \bmod q}}^{h} 1 - \frac{h}{2^{\omega(q)}P}\right)^2 \le \frac{q}{4^{\omega(q)}P}h\prod_{p|q}(2+\frac{2p^{3/2}-p-1}{p^2+2p+1}) < \frac{q}{2^{\omega(q)}P}h\prod_{p|q}(1+\frac{1}{\sqrt{p}}).$$

For the lower bound, let $r > h^2$. Then we have

$$\phi(r)h \ll \sum_{\substack{a<r\\ (a,r)=1}}\left|E\left(\frac{a}{r}\right)\right|^2.$$

Therefore,

$$\frac{q}{4^{\omega(q)}P}h\sum_{\substack{r>h^2\\ r|q}}\prod_{p|r}(1-\frac{3}{\sqrt{p}}) \ll \sum_{n=0}^{q-1}\left(\sum_{\substack{m=1\\ n+m \text{ is } \square \bmod q}}^{h} 1 - \frac{h}{2^{\omega(q)}P}\right)^2.$$

$\square$

Proof of Corollary 2.6. Let

$$L(x) = \#\left\{i : 1 \le i \le \prod_{p|q}\left(\frac{p+1}{2}\right) \text{ and } s_{i+1} - s_i > x\right\}.$$

Then

$$\sum_{s_i<q}(s_{i+1}-s_i)^2 = 2\int_0^{\infty} L(y)y\,dy. \tag{2.39}$$

For $y < 2^{\omega(q)}P^{-1}\log q\prod_{p|q}(1+\frac{1}{\sqrt{p}})$ we bound (2.39) trivially. To bound $L(y)$ we note that if $s_{i+1} - s_i > h$, then

$$\sum_{\substack{m=1\\ n+m \text{ is } \square \bmod q}}^{h} 1 - \frac{h}{2^{\omega(q)}P} = -\frac{h}{2^{\omega(q)}P},$$

for $s_i \le n \le s_{i+1} - h$. Therefore we have

$$\sum_{s_{i+1}-s_i>h}(s_{i+1}-s_i-h)\left(\frac{h}{2^{\omega(q)}P}\right)^2 \ll \sum_{n=0}^{q-1}\left(\sum_{\substack{m=1\\ n+m \text{ is } \square \bmod q}}^{h} 1 - \frac{h}{2^{\omega(q)}P}\right)^2. \tag{2.40}$$

Now if we take $y = [h/2]$ then the left hand side of (2.40) is

$$\gg L(y)y\left(\frac{y}{2^{\omega(q)}P}\right)^2.$$

Thus, by employing Theorem 2.2 we get the following bound:

$$L(y) \ll \frac{2^{\omega(q)}P}{y^2}\prod_{p|q}(1+\frac{1}{\sqrt{p}}).$$

Applying this bound in the integral in (2.39) and the fact that for $y > q$, $L(y) = 0$ completes the proof of the Corollary. $\qquad \square$

2.4 The general case

In this section we will prove Theorems 2.12, 2.18 and 2.20. Let $\Omega_p \subset \mathbb{Z}/p\mathbb{Z}$. We are interested in numbers less than q such that, modulo p, they do not occupy any congruence classes in Ω_p, i.e. $\{m \leq q : m \notin \Omega_p \bmod p\}$. By the Chinese Remainder Theorem there exist $\prod_{p|q}(p - |\Omega(p)|)$ such numbers. A natural question is to ask about their distribution modulo q (see [29]). Lemma 2.23 shows the connection between the distribution of these numbers and the exponential sum over elements in Ω_p. Let $\mathcal{D} = \{h_1, \ldots, h_s\}$ be a set such that $\mathcal{D}_p = \{-\omega : \omega \in \Omega_p\}$. If $k_q(m+h_1) \ldots k_q(m+h_s) = 1$, then m is not congruent to any member of Ω_p modulo p. Now we take a look at the distribution of these numbers. Observe that

$$\sum_{m=1}^{h}k_q(m+h_1)\ldots k_q(m+h_s)$$

$$= \prod_{p|q}\frac{p-|\Omega_p|}{p}\sum_{r|q}\frac{\mu(r)}{\prod_{p|r}(p-|\Omega_p|)}\sum_{\substack{a<r\\(a,r)=1}}E\left(\frac{a}{r}\right)\mu_{\mathcal{D}}(a,r). \qquad (2.41)$$

By a calculation similar to (2.31) we have

$$\sum_{n=0}^{q-1}\left(\sum_{m=1}^{h} k_q(n+m+h_1)\ldots k_q(n+m+h_s) - h\prod_{p|q}\left(\frac{p-|\Omega_p|}{p}\right)\right)^2 \qquad (2.42)$$

$$= q\prod_{p|q}\left(\frac{p-|\Omega_p|}{p}\right)^2 \sum_{\substack{r|q\\r>1}}\frac{1}{\prod_{p|r}(p-|\Omega_p|)^2}\sum_{\substack{0<a\le r\\(a,r)=1}}\left|E\left(\frac{a}{r}\right)\mu_{\mathcal{D}}(a,r)\right|^2.$$

In the next lemma we bound the variance.

Lemma 2.24. *Assume that for each $p|q$, $|\Omega_p| = c'_p p$ with $(p-|\Omega_p| > p^{1/2+\varepsilon})$, and $|\mu_{\mathcal{D}}(a,p)| <$*
$c_p\sqrt{p}$, *where $c'_p < 1$. Then we have that*

$$\sum_{n=0}^{q-1}\left(\sum_{\substack{m\in[n,n+h]\\m\notin\Omega_p\bmod p\\\forall p|q}} 1 - h\prod_{p|q}\left(\frac{p-|\Omega_p|}{p}\right)\right)^2 \le qh\prod_{p|q}\left((1-c'_p)^2 + c_p^2\right).$$

Proof. Using the assumptions in Lemma 2.24 and (2.38) we have

$$\sum_{n=0}^{q-1}\left(\sum_{m=1}^{h} k_q(n+m+h_1)\ldots k_q(n+m+h_s) - h\prod_{p|q}\left(\frac{p-|\Omega_p|}{p}\right)\right)^2$$

$$\ll q\prod_{p|q}\left(\frac{p-c'_p p}{p}\right)^2 \sum_{\substack{r|q\\r>1}}\frac{h\prod_{p|r}(c_p p)^2}{\prod_{p|r}(p-c'_p p)^2} = qh\prod_{p|q}(1-c'_p)^2 \sum_{\substack{r|q\\r>1}}\prod_{p|r}\left(\frac{c_p}{1-c'_p}\right)^2$$

$$< qh\prod_{p|q}(1-c'_p)^2\left(1+\left(\frac{c_p}{1-c'_p}\right)^2\right) = qh\prod_{p|q}\left((1-c'_p)^2 + c_p^2\right).$$

This completes the proof of the lemma.

$\square$

Proof of Theorem 2.12. This follows from Lemma 2.24 by taking $c'_p = (p-1)/2p$. Recall
that $c'_p = \frac{|\Omega_p|}{p}$. $\qquad\square$

Next we prove Theorem 2.18:

Proof of Theorem 2.18. . Let $\mathcal{D}^* = \{h_1, \ldots, h_s\}$ be an admissible set such that $\mathcal{D}_p^* = -\Omega_p = \{0, -2, \ldots, -(p-1)\}$. Let $\dfrac{a}{r} = \sum_{p|r} \dfrac{a_p}{p}$, for $a_p = \dfrac{p \pm 1}{2}$. Since $\mathcal{D}_p^* = \{0, 2, \ldots, p-1\}$, applying Lemma 2.23 we have that

$$|\mu_{\mathcal{D}^*}(a,r)| = \prod_{p|r} \left| \sum_{s \in \mathcal{D}_p^*} e\left(\frac{sa_p}{p}\right) \right| = \prod_{p|r} \left| \frac{e\left(\frac{1}{2p}\right)+1}{e\left(\frac{1}{p}\right)-1} \right| \geq \prod_{p|r} \frac{p}{\pi}. \tag{2.43}$$

Here, similar to the square case (section 2), we have $P_{\mathcal{D}^*} = \dfrac{1}{2^{\omega(q)}} P$ and $\phi_{\mathcal{D}^*}(r) = \prod_{p|r} \dfrac{p-1}{2}$.
Consequently, using (2.43) we have, similarly to (2.29) and (2.32), that

$$\sum_{n=0}^{q-1} \left(\sum_{m=1}^{h} k_q(n+m+h_1) \ldots k_q(n+m+h_s) - \frac{hP}{2^{\omega(q)}} \right)^2$$

$$= \frac{qP^2}{2^{2\omega(q)}} \sum_{\substack{r|q \\ r>1}} \left(\frac{1}{\left(\prod_{p|r} \frac{p-1}{2}\right)^2} \right) \sum_{\substack{0<a\leq r \\ (a,r)=1}} \left| E\left(\frac{a}{r}\right) \mu_{\mathcal{D}^*}(a,r) \right|^2$$

$$\geq \frac{qP^2}{2^{2\omega(q)}} \sum_{\substack{r|q \\ r>1}} \frac{4^{\omega(r)}}{\phi(r)^2} \sum_{\substack{a_p=\frac{p\pm 1}{2} \\ p|r}} \left| E\left(\sum_{p|r} \frac{a_p}{p}\right) \mu_{\mathcal{D}^*}(a,r) \right|^2$$

$$\geq \frac{qP^2}{2^{2\omega(q)}} \sum_{\substack{r|q \\ r>1}} \frac{4^{\omega(r)}r^2}{\phi(r)^2\pi^{2\omega(r)}} \sum_{p|r} \left| E\left(\sum_{p|r} \frac{1}{2} \pm \frac{1}{2p}\right) \right|^2. \tag{2.44}$$

Now, for r with an even number of distinct prime factors and $\left\| \sum_{p|r} \dfrac{\pm 1}{p} \right\| \ll 1/h$, where $\|\cdot\|$ denotes the distance to the nearest integer, we have

$$\left| E\left(\sum_{p|r} \frac{1}{2} \pm \frac{1}{2p}\right) \right|^2 \gg h^2.$$

Consequently (2.44) is

$$\gg \frac{qP^2}{2^{2\omega(q)}} h^2 \sum_{\substack{r|q \\ r>1 \\ \|\sum_{p|r}\frac{\pm 1}{p}\| \ll 1/h}} \frac{4^{\omega(r)}r^2}{\phi(r)^2\pi^{2\omega(r)}}.$$

Now let $r = p_1 p_2$, with $a_{p_1} = \dfrac{p_1 + 1}{2}$ and $a_{p_2} = \dfrac{p_2 - 1}{2}$, we have

$$\| \frac{p_1 + 1}{2p_1} + \frac{p_2 - 1}{2p_2} \| = \| \frac{1}{2p_1} - \frac{1}{2p_2} \| \ll \left| \frac{\log X}{X^2} \right| \ll \frac{1}{h},$$

which implies that (2.44) is

$$\gg \frac{qP^2}{2^{2\omega(q)}} h^2.$$

$\square$

Remark 2.25. We picked $h = \frac{X^2}{\log X}$, so that the expectation of

$$\#\{m \in (n, n+h] : m \notin \mathcal{D}_p^* \bmod p, \text{ for all } \; p|q\} = h \prod_{p|q} \frac{p+1}{2p} = \frac{X^2 P}{2^{\lfloor \log X \rfloor} \log X}$$

is greater than 1. This is important in order to have the possibility of cancellation inside

$$\sum_{n=0}^{q-1} \left(\sum_{m=1}^{h} k_q(n+m+h_1) \ldots k_q(n+m+h_s) - \frac{hP}{2^{\omega(q)}} \right)^2 .$$

We complete this section with the proof of Theorem 2.20.

Proof of Theorem 2.20. We begin with giving the proof for equation (2.19). Recall that

$$\Omega'_{K,p} := \left\{ x + x^{-1} : 1 \leq x, x^{-1} \leq p - 1 \text{ and } x +_{\mathbb{Z}} x^{-1} < p \right\},$$

If $x +_{\mathbb{Z}} x^{-1} < p$ then $(p - x) +_{\mathbb{Z}} (p - x)^{-1} \geq p$, Therefore half of the congruence classes modulo p contribute to the size of $\Omega'_{K,p}$. Also, for $y < p$ we have $x +_{\mathbb{Z}} x^{-1} = x^{-1} +_{\mathbb{Z}} x = y$. This means that each $y \in \Omega'_{K,p}$ has a double multiplicity, with the exception of y equal to $1 + 1^{-1}$. Considering the fact that for $p \equiv 1 \bmod 4$, there exists an x such that $x^{-1} = p - x$, and therefore $x + x^{-1} = p$. This completes the proof of equation (2.19).

Now let $\Omega_p := \left\{ -\omega : \omega \in \{0, 1, \ldots, p-1\} \setminus \Omega'_{K,p} \right\} = \{\omega_1, \ldots, \omega_{|\Omega_p|}\}$. Using (2.19) we

have $|\Omega_p| = \frac{3}{4}p + O(\frac{1}{p})$. If $k_p(m+\omega_1)k_p(m+\omega_2)\ldots k_p(m+\omega_{|\Omega_p|}) = 1$, then $m \in \Omega_{K,p}$. We

use (2.42) to transform the left hand side of (2.20), and we have

$$
\frac{1}{p}\sum_{n=0}^{p-1}\left(\sum_{\substack{m\in[n,n+h]\\m\in\Omega'_{K,p}}} 1 - \frac{h}{p}|\Omega'_{K,p}|\right)^2 \gg \frac{1}{p^2}\sum_{0<a\leq p-1}\left|E\left(\frac{a}{p}\right)\mu_{\Omega_p}(a,p)\right|^2. \tag{2.45}
$$

To finish the proof of the theorem it is enough to show that $\left|E\left(\frac{1}{p}\right)\mu_{\Omega_p}(1,p)\right| \gg hp$. Since

$h < p/2$ we have that $\left|E\left(\frac{1}{p}\right)\right| \gg h$. For μ_{Ω_p} we have

$$
\mu_{\Omega_p}(1,p) = \sum_{x\in\Omega_p} e\left(\frac{x}{p}\right).
$$

Recall that $\Omega_{K,p}, \Omega'_{K,p}$ are defined by (2.12) and (2.15). Therefore if $-\omega \in \Omega_p$ then $\omega \in$

$\left(\mathbb{Z}/p\mathbb{Z}\setminus\Omega_{K,p}\right)\cup\{x+x^{-1}:x+_\mathbb{Z}x^{-1}\geq p\}$. We have

$$
\mu_{\Omega_p}(1,p) = \sum_{x\in\mathbb{Z}/p\mathbb{Z}\setminus\Omega_{K,p}} e\left(\frac{-x}{p}\right) + \sum_{\omega\in\{x+x^{-1}:x+_\mathbb{Z}x^{-1}\geq p\}} e\left(\frac{-\omega}{p}\right).
$$

Using Weil's bound for Kloosterman sums, the first sum above is $O(\sqrt{p})$. For the second

sum we prove

$$
\sum_{\omega\in\{x+x^{-1}:x+_\mathbb{Z}x^{-1}\geq p\}} e\left(\frac{-\omega}{p}\right) = \frac{ip}{2\pi} + O(\sqrt{p}\log p). \tag{2.46}
$$

The following argument for (2.46) was given by Will Sawin and Noam Elkies on Math

Overflow [1]. The left hand side of (2.46) is equal to

$$
\sum_{1\leq x,y\leq p-1} \mathbf{1}_{\{xy=1\}}e\left(\frac{-x-y}{p}\right)\mathbf{1}_{\{x+_\mathbb{Z}y\geq p\}}.
$$

We use a two dimensional Fourier transform to evaluate the left hand side of (2.46). Let

$\hat{A}(a,b)$ be the Fourier transform of $\mathbf{1}_{\{xy=1\}}$ and $\hat{B}(a,b)$ be the Fourier transform of $\mathbf{1}_{\{x+y>p\}}e\left(\frac{x+y}{p}\right)$.

Then by using Parseval-Plancherel formula, the sum in (2.46) is:

$$\frac{\sum_{0 \le a, b \le p-1} \hat{A}(a,b) \overline{\hat{B}(a,b)}}{p^2}, \tag{2.47}$$

where

$$\hat{A}(a,b) = \sum_{0 \le x < p} e\left(\frac{ax + bx^{-1}}{p}\right) = S(a,b;p),$$

$$\hat{B}(a,b) = \sum_{\substack{0 \le x,y < p \\ x+y>p}} e\left(\frac{(a-1)x + (b-1)y}{p}\right).$$

Note that $\hat{A}(a,b)$ is the Kloosterman sum unless $a = b = 0$. For $\hat{B}(a,b)$ when $b \ne 1$ we have

$$
\begin{aligned}
\hat{B}(a,b) &= \sum_{1 \le x < p} e\left(\frac{(a-1)x}{p}\right) \left(\sum_{p+1-x \le y \le p-1} e\left(\frac{(b-1)y}{p}\right) \right) \\
&= \sum_{1 \le x < p} e\left(\frac{(a-1)x}{p}\right) \frac{e(b-1) - e\left(\frac{(b-1)(1-x)}{p}\right)}{e\left(\frac{b-1}{p}\right) - 1} \\
&= \sum_{1 \le x < p} \left(\frac{e\left(\frac{(a-1)x}{p}\right)}{e\left(\frac{b-1}{p}\right) - 1} - \frac{e\left(\frac{(a-b)x+b-1)}{p}\right)}{e\left(\frac{b-1}{p}\right) - 1} \right).
\end{aligned}
$$

The first term in the latter sum is $\frac{p-1}{e((b-1)/p)-1)}$ if $a = 1$ and $\frac{-1}{e((b-1)/p)-1}$ otherwise. The second term in the latter sum is $\frac{(p-1)e((b-1)/p)}{e((b-1)/p)-1}$ if $a = b$ and $\frac{-e((b-1)/p)}{e((b-1)/p)-1)}$ otherwise.

Note that if $a = b = 1$, then $\hat{B}(1,1)$ is $(p-1)(p-2)/2$. Also if $b = 1$ and $a \ne 1$ we have

$$\hat{B}(a,b) = \frac{p}{e\left(\frac{a-1}{p}\right) - 1} + 1 \ll \frac{p^2}{a}.$$

Now the main term in (2.47) comes from the contribution of $\hat{A}(0,0) \overline{\hat{B}(0,0)}$. The error term can be handled by using the Weil bound on $\hat{A}(a,b)$ for $(a,b) \ne (0,0)$ and the above elementary estimates for $\overline{\hat{B}(a,b)}$ for $(a,b) \ne (1,1)$. $\qquad \square$

2.5 Higher central moments of reduced residues modulo q

In this section we will improve the result in [3] regarding the higher central moments of s-tuples of reduced residues. The improvement comes from using Lemma 2.23 to transform characteristic functions of s-tuples of reduced residues to an expression in terms of exponential sums. The rest of the proof will follow Montgomery and Vaughan's [60] arguments (Lemma 7 and 8 in [60]). The important part of the proof is to estimate the innermost sum in (2.48), which we divide into two cases: diagonal and non-diagonal configurations. In the diagonal configuration the estimate derived is good enough for our purposes. In the non-diagonal configuration we use Lemma 7 and 8 in [60] to save a small power of h. Let $\mathcal{D} = \{h_1, \ldots, h_s\}$ be a fixed admissible set. By employing Lemma 2.23 we have that

$$
\sum_{n=0}^{q-1} \left(\sum_{m=1}^{h} k_q(n+m+h_1)\ldots k_q(n+m+h_s) - hP_{\mathcal{D}} \right)^k
$$
$$
= qP_{\mathcal{D}}^k \sum_{\substack{r_i|q \\ r_i>1}} \left(\prod_{i=1}^{k} \frac{\mu(r_i)}{\phi_{\mathcal{D}}(r_i)} \right) \sum_{\substack{0<a_i\leq r_i \\ (a_i,r_i)=1 \\ \sum_{i=1}^{k}\frac{a_i}{r_i}\in\mathbb{Z}}} \left(E\left(\frac{a_1}{r_1}\right)\mu_{\mathcal{D}}(a_1,r_1)\ldots E\left(\frac{a_k}{r_k}\right)\mu_{\mathcal{D}}(a_k,r_k) \right),
$$

where

$$
\mu_{\mathcal{D}}(a,r) = \prod_{p|r} \left(\sum_{\substack{s\equiv h_i \bmod p \\ h_i\in\mathcal{D}}} e\left(\frac{sa(r/p)_p^{-1}}{p}\right) \right).
$$

Let $F(x) = \min(h, \frac{1}{\|x\|})$ where $\|x\|$ is the distance between x and the closest integer to x. We have that $|E(x)| \leq F(x)$. Since $|\mu_{\mathcal{D}}(a,r)| \leq s^{\omega(r)}$ we have

$$
M_k^{\mathcal{D}}(q,h) \ll qP_{\mathcal{D}}^k \sum_{r|q} \sum_{\substack{r_i|r \\ r_i>1 \\ [r_1,\ldots r_k]=r}} \prod_{i=1}^{k} \frac{s^{\omega(r_i)}}{\phi_{\mathcal{D}}(r_i)} \sum_{\substack{0<a_i\leq r_i \\ (a_i,r_i)=1 \\ \sum_{i=1}^{k}\frac{a_i}{r_i}\in\mathbb{Z}}} F\left(\frac{a_1}{r_1}\right)\ldots F\left(\frac{a_k}{r_k}\right). \tag{2.48}
$$

Proof of Theorem 2.21. We use the method in [60] to bound

$$\sum_{\substack{0<a_i\leq r_i \\ (a_i,r_i)=1 \\ \sum_{i=1}^{k}\frac{a_i}{r_i}\in\mathbb{Z}}} F\left(\frac{a_1}{r_1}\right)\ldots F\left(\frac{a_k}{r_k}\right)$$

in (2.48). First we focus on diagonal configuration i.e. $r_1=r_2, r_3=r_4,\ldots,r_{k-1}=r_k$ and $r_2,r_4,\ldots,r_k$ are relativity co-prime. In the diagonal configuration we have that

$$\sum_{\substack{0<a_i\leq r_i \\ (a_i,r_i)=1 \\ \sum_{i=1}^{k}\frac{a_i}{r_i}\in\mathbb{Z}}} F\left(\frac{a_1}{r_1}\right)\ldots F\left(\frac{a_k}{r_k}\right) \leq \sum_{0<a_1\leq r_1} F\left(\frac{a_1}{r_1}\right)^2 \ldots \sum_{0<a_{k-1}\leq r_{k-1}} F\left(\frac{a_{k-1}}{r_{k-1}}\right)^2$$

$$\leq r_1 r_3\ldots r_{k-1} h^{k/2} = [r_1 r_3 \ldots r_{k-1}] h^{k/2}.$$

Consequently, the contribution of the the diagonal configuration in (2.48) is less than

$$qP_{\mathcal{D}}^k \sum_{r|q} \sum_{\substack{[r_1,\ldots,r_k]=r \\ (r_{2i-1},r_{2j-1})=1 \\ i\neq j}} \left(r_1\frac{s^{2\omega(r_1)}}{\phi_{\mathcal{D}}(r_1)^2}\right)\left(r_3\frac{s^{2\omega(r_3)}}{\phi_{\mathcal{D}}(r_3)^2}\right)\cdots\left(r_{k-1}\frac{s^{2\omega(r_{k-1})}}{\phi_{\mathcal{D}}(r)^2}\right) h^{k/2}$$

$$= qP_{\mathcal{D}}^k \sum_{r|q} \left(r\frac{(s^2\frac{k}{2})^{\omega(r)}}{\phi_{\mathcal{D}}(r)^2}\right) h^{k/2} = qP_{\mathcal{D}}^k \prod_{p|q}\left(1+\frac{ps^2\frac{k}{2}}{\left(p-\nu_p(\mathcal{D})\right)^2}\right) h^{k/2}$$

$$\ll qh^{k/2}P^{sk-s^2\frac{k}{2}}. \tag{2.49}$$

In (2.49) we used the fact that the number of k-tuples $(r_1,\ldots,r_k)$ with $[r_1,\ldots,r_k]=r$ such that each p divides exactly two of r_i is less than $(k/2)^{\omega(r)}$ (see [61]). In the non-diagonal configuration Lemma 7 in [60] allows us to save a small power of h. Now we state the Lemma 7 in [60] and explain how it should be apply. Our aim is to get the following

$$M_k^{\mathcal{D}}(q,h) \ll qh^{k/2}P^{sk-s^2\frac{k}{2}}\left(1+h^{-\frac{1}{7k}}P^{-(s+1)^k}\right). \tag{2.50}$$

This bound is analogous to [60, Lemma 8] and its proof is nearly identical. The key dif-

ference is in (2.48) we have $s^{\omega(r)}/\phi_{\mathcal{D}(r)}$ instead of $1/\phi(r)$. Our main tool is the following lemma.

Lemma 2.26 (Montgomery and Vaughan). *For $k \geq 3$, let $r_1, \ldots, r_k$ be square free numbers with $r_i \geq 1$ for all i. Further let $r = [r_1, r_2, \ldots, r_k]$, $d = (r_l, r_2)$, $r_1 = dr'_1, r_2 = dr'_2$. and write $d = st$ where $s \mid r_3 \ldots r_k$, $(t, r_3 r_4 \ldots r_k) = 1$. Then*

$$\sum_{\substack{0 < a_i \leq r_i \\ (a_i, r_i) = 1 \\ \sum_{i=1}^{k} \frac{a_i}{r_i} \in \mathbb{Z}}} F\left(\frac{a_1}{r_1}\right) \ldots F\left(\frac{a_k}{r_k}\right) \ll r_1 \ldots r_k r^{-1}(T_1 + T_2 + T_3 + T_4) \tag{2.51}$$

where

$$T_1 = h^{-1/20};$$

$$T_2 = d^{-1/4} \text{ when } r_i > h^{8/9} \text{ for all } i,$$

$$T_2 = 0 \text{ otherwise;}$$

$$T_3 = s^{-1/2} \text{ when } r_i > h^{8/9} \text{ for all } i \text{ and } r_1 = r_2,$$

$$T_3 = 0 \text{ otherwise;}$$

and

$$T_4 = \left(\frac{1}{r_1 r_2 s h^2} \sum_{(\tau, t) = 1} F\left(\frac{\| r'_1 s\tau \|}{r'_1 s}\right)^2 F\left(\frac{\| r'_2 s\tau \|}{r'_2 s}\right)^2\right)^{1/2}$$

when $h^{8/9} < r_i \leq h^2$ for $i = 1, 2, t > d^{1/2}$ and $d < h^{5/9}$,

$$T_4 = 0 \text{ otherwise.}$$

We shall also use the following estimate [60, Lemma 1]

$$\sum_{\substack{0 < a_i \leq r_i \\ (a_i, r_i) = 1 \\ \sum_{i=1}^{k} \frac{a_i}{r_i} \in \mathbb{Z}}} F\left(\frac{a_1}{r_1}\right) \dots F\left(\frac{a_k}{r_k}\right) \ll \frac{1}{r} \prod_{i=1}^{k} \left(r_i \sum_{(a_i, r_i) = 1} F\left(\frac{a_i}{r_i}\right)^2 \right)^{1/2}. \tag{2.52}$$

Now we explain how to choose r_1, r_2 in order to apply Lemma 2.26. Note that we only need to consider those k-tuples $r = (r_1, r_2, , \dots, r_k)$ for which $r_i > 1, [r_1, \dots, r_k] = r$, and each prime divisor of r divides at least two of the r_i, since otherwise the sum on the left hand side of (2.51) is empty. If $r_i < h^{8/9}$ for some i, then by using (2.52) and [60, Lemma 4] we have our desired result. Now suppose that $r_i > h^{8/9}$ for all i, and set $d_{ij} = (r_i, r_j)$. For each i we can find a j, such that

$$d_{i,j} \geq h^{8/(9k-9)}. \tag{2.53}$$

If there is a pair (i, j) for which this holds and $r_i \neq r_j$, then in Lemma 2.26 we choose these to be r_1, r_2. We note that if $r_i = r_1$ then $d_{i,j} = r_i > h^{8/9}$, and (2.53) holds. Suppose now that (2.53) holds only when $r_i = r_j$. If there is a triple (i, j, k) such that $r_i = r_1 = r_k$, then we apply Lemma 2.26 with r_i, r_j as r_1, r_2. Otherwise the r_i are equal in distinct pairs, say $r_1 = r_2, r_3 = r_4, \dots, r_{k-l} = r_k$, and k is even. Let v be the product of all those prime factors of r which divide more than one of the numbers $r_2, r_4, r_6, \dots, r_k$. Then there exists i such that

$$\left(r_{2i}, \prod_{j \neq i} r_{2j} \right) \geq v^{4/k}. \tag{2.54}$$

In this case we take r_1 and r_2 to be r_{2i-1}, r_{2i} and by employing Lemma 2.26 we have

$$M_k^{\mathcal{D}}(q, h) \ll q P_{\mathcal{D}}^k \sum_{r | q} \frac{1}{r} \sum_{\substack{r_i | r \\ r_i > 1 \\ [r_1, \dots r_k] = r}} \prod_{i=1}^{k} \frac{s^{\omega(r_i)} r_i}{\phi_{\mathcal{D}}(r_i)} \left(T_1 + T_2 + T_3 + T_4 \right). \tag{2.55}$$

Note that if any of T_2, T_3, or T_4 is non-zero then $d \geq h^{8/(9k-9)}$. The contribution of T_1 to

(2.55) is

$$\ll qP^{sk} \prod_{p|q} \left(1 + \frac{\left(1 + sp/\phi_{\mathcal{D}}(p)\right)^k}{p}\right) \ll qP^{sk-(s+1)^k} h^{-1/20}. \tag{2.56}$$

By the selection of r_1, r_2 we have that if $T_2 \neq 0$ then $d \geq h^{8/(9k-9)}$. Therefore the contribution of T_2 to (2.55) is $\ll qP^{sk-(s+1)^k} h^{-2/(9k-9)}$. Now for T_3 we have $r_1 = r_2$ and $r_1 \geq h^{8/9}$. If $r_1 = r_2 = r_i$ for some $i > 2$, then $s = r > h^{8/9}$, so that $T_3 < T_1$ and therefore the contribution of such T_3 to (2.55) is smaller than T_1. It remains to consider the case when $r_1 = r_2, r_3 = r_4, \ldots, r_{k-1} = r_k$. Let $r = uv$ where u is the product of those primes dividing exactly one of $r_2, r_4, \ldots, r_k$. Then each prime divisor of v divides two or more of the r_{2i}. By our choice of r_1, r_2 we have $s \geq v^{4/k}$. Put $r_i = u_i v_i$ where $u_i = (r_i, u)$ and $v_i = (r_i, v)$. Suppose that u and v are fixed, and let $C(u, v)$ denote the set of $(r_1, \ldots, r_k)$ of the sort under consideration. We have $|C(u, v)| \leq d_{k/2}(u) d(v)^{k/2}$. Using the change of variable $r = uv$ and by rearranging the sum in (2.55), for the contribution of T_3 we have

$$\sum_{uv|q} \frac{1}{uv} \sum_{(r_1,\ldots,r_k) \in C(u,v)} \left(\prod \frac{s^{\omega(r_i)} r_i}{\phi_{\mathcal{D}}(r_i)}\right) T_3 \ll \sum_{uv|q} \frac{d_{k/2}(u)\left(\frac{s^{\omega(u)} u}{\phi_{\mathcal{D}}(u)}\right)^2 d(v)^{k/2}\left(\frac{s^{\omega(v)} v}{\phi_{\mathcal{D}}(v)}\right)^k}{uv^{1+2/k}} \tag{2.57}$$

$$= \prod_{p|q} \left(1 + \frac{ks^2 p}{2\phi_{\mathcal{D}}^2(p)} + \frac{2^{k/2}\left(sv/\phi_{\mathcal{D}}(p)\right)^k}{p^{1+2/k}}\right)$$

$$\ll P^{-\frac{s^2 k}{2}}.$$

For the contribution of T_4, by the Cauchy inequality, we have

$$\sum_{r|q} \frac{1}{r} \sum_{\substack{r_i|r \\ r_i>1 \\ [r_1,\ldots r_k]=r}} \prod_{i=1}^{k} \frac{s^{\omega(r_i)} r_i}{\phi_{\mathcal{D}}(r_i)} T_4 \ll \left(\sum_{r|q} \frac{1}{r} \sum_{r_1,\ldots,r_k} \left(\prod \frac{s^{\omega(r_i)} r_i}{\phi_{\mathcal{D}}(r_i)}\right)^2\right)^{1/2} \left(\sum_{r|q} \frac{1}{r} \sum_{r_1,\ldots,r_k} T_4^2\right)^{1/2}.$$

$$\tag{2.58}$$

The first factor on the right is made larger as it runs over all k-tuples for which $r_i|r$. The

larger expression is

$$\sum_{r|q} \frac{1}{r} \prod_{p|r} \left(1 + \left(\frac{sp}{\phi_{\mathcal{D}}(p)}\right)^2\right)^k = \prod_{p|q} \left(1 + \frac{\left(1 + \left(\frac{sp}{\phi_{\mathcal{D}}(p)}\right)^2\right)^k}{p}\right) \ll P^{-(s^2+1)^k}. \tag{2.59}$$

The second factor has been treated precisely in [60, pp. 324-325] and it is smaller than $h^{-2/7k}$. By combining (2.56), (2.57), (2.58) and (2.59) we complete the proof of (2.50). Note that we have just sketched the key ideas of the proof, the interested reader can find further details in [60]. To finish the proof of the Theorem 2.21 we appeal to Lemma 3.1 in [3]. Let $q_1 = \prod_{\substack{p|q \\ p \leq y}} p$ and $q_2 = \prod_{\substack{p|q \\ p > y}} p$, where $y \geq h^k$. We set $P_i = \frac{\phi(q_i)}{q_i}$ for $i = 1, 2$. Then [3, Lemma 3.1] states that

$$M_k^{\mathcal{D}}(q, h) \ll q(hP^s)^{[k/2]} + qh(P)^s + qh^{k/2} P_1^{-2ks+ks} P_2^{sk}.$$

This lemma is obtained by combining two different estimates of $M_k^{\mathcal{D}}(q, h)$: an exponential estimate and a probabilistic estimate. The exponential estimate stated in [3, Lemma 1.2] gives

$$M_k^{\mathcal{D}}(q, h) \ll qh^{k/2} P^{-2ks+ks}.$$

Here we use the estimate (2.50), instead of the above estimate and we derive:

$$M_k^{\mathcal{D}}(q, h) \ll_k q(hP^s)^{[k/2]} + qhP^s + qh^{k/2} P_1^{sk-s^2\frac{k}{2}} \left(1 + h^{-\frac{1}{7k}} P_1^{-(s+1)^k}\right) P_2^{sk}.$$

Now by considering $y = h^k$, we have (2.25) and for $h < e^{\frac{1}{kP^{1/s}}}$, we have (2.24), which completes the proof. □

'

Chapter 3

Discrete mean values of Dirichlet polynomials

3.1 Introduction.

Let $a, b : \mathbb{Z} \to \mathbb{C}$ be arithmetic sequences such that

$$\text{supp}(a) \subseteq [1, M] \text{ and } \text{supp}(b) \subseteq [1, N], \tag{3.1}$$

where $M, N \geq 1$ [1]. Furthermore, we impose the size conditions

$$a(n) = O_\varepsilon(n^\varepsilon) \text{ and } b(n) = O_\varepsilon(n^\varepsilon). \tag{3.2}$$

For every $\varepsilon > 0$. Attached to a and b are the Dirichlet polynomials

$$
\begin{aligned}
A(s) &= \sum_n \frac{a(n)}{n^s} = \sum_{n \leq M} \frac{a(n)}{n^s}, \\
B(s) &= \sum_n \frac{b(n)}{n^s} = \sum_{n \leq N} \frac{b(n)}{n^s}.
\end{aligned}
\tag{3.3}
$$

A key tool in analytic number theory is an estimate for

$$\int_{-T}^{T} A(\tau_1 + it) B(\tau_2 - it) dt, \text{ where } \tau_1, \tau_2 \in \mathbb{R}. \tag{3.4}$$

---

[1] For $x : \mathbb{Z} \to \mathbb{C}$, $\text{supp}(x) = \{ n \in \mathbb{Z} \mid x(n) \neq 0 \}$.

A theorem of Montgomery and Vaughan [59] implies that

$$\int_{-T}^{T} A(\tau_1 + it)B(\tau_2 - it)dt = \sum_{n \leq N} \frac{a(n)b(n)}{n^{\tau_1 + \tau_2}}(2T + O(N)).$$

If $N = o(T)$, then the mean value is asymptotic to $\sum_{n \leq N} a(n)b(n)n^{-\tau_1 - \tau_2}$. However, if $N \gg T$, then the behaviour of this sum changes. Indeed, the "main term" will no longer just involve $\sum_{n \leq N} a(n)b(n)$. In fact, it is necessary to consider correlations of $a(n)$ and $b(n)$. We now introduce the correlation functions. Let $a, b : \mathbb{N} \to \mathbb{C}$ be arithmetic functions and $h \in \mathbb{Z}$. For a triple $(a, b; h)$ we define a correlation function by

$$\mathscr{C}_{a,b;h}(x) = \sum_{n \leq x} a(n)b(n+h). \tag{3.5}$$

Note that we define this when $h \in \mathbb{Z}$. In the case $h = 0$ we have

$$\mathscr{C}_{a,b}(x) := \mathscr{C}_{a,b;0}(x) = \sum_{n \leq x} a(n)b(n), \tag{3.6}$$

and when $h < 0$, we have

$$\mathscr{C}_{a,b;h}(x) = \sum_{|h|+1 \leq n \leq x} a(n)b(n+h), \tag{3.7}$$

since $b(n) = 0$ for $n \leq 0$. Throughout this chapter we suppose that these correlation functions satisfy the following nice property. There exist functions $\mathscr{M}_{a,b;h}(x)$ and $\mathscr{E}_{a,b;h}(x)$ such that

$$\mathscr{C}_{a,b;h}(x) = \mathscr{M}_{a,b;h}(x) + \mathscr{E}_{a,b;h}(x) \tag{3.8}$$

where $\mathscr{M}_{a,b;h}(x)$, the "main term", is a differentiable function of x and $\mathscr{E}_{a,b;h}(x)$ is an "error term." Moreover, we require a uniform bound of the following shape on $\mathscr{E}_{a,b}(x, h)$: there

exists $\vartheta := \vartheta(a,b)$ and $\delta := \delta(a,b)$ such that for any $\varepsilon > 0$

$$\mathcal{E}_{a,b}(x,h) \ll x^{\vartheta+\varepsilon} \text{ for all } |h| \leq x^{\delta}. \tag{3.9}$$

In the case $h = 0$, we shall write this as

$$\mathcal{C}_{a,b}(x) = \mathcal{C}_{a,b;0}(x) = \mathcal{M}_{a,b}(x) + \mathcal{E}_{a,b}(x). \tag{3.10}$$

It shall be convenient to consider a weighted sum of the form

$$I = I_{a,b,\tau_1,\tau_2,\omega} := \int_{\mathbb{R}} \omega(t) A(\tau_1 + it) B(\tau_2 - it) dt \tag{3.11}$$

where $\tau_1, \tau_2 \in \mathbb{R}$, and ω is a complexed valued function defined over $\mathbb{R}$. Attached to ω, we define its Fourier transform

$$\widehat{\omega}(\xi) = \int_{\mathbb{R}} \omega(t) e^{-2\pi i \xi t} dt. \tag{3.12}$$

Note that $\widehat{\omega}(0) = \int_{-\infty}^{\infty} \omega(t) dt$, is the total weight of ω. Swapping summation order with the integral in (3.11), we have

$$I = \sum_{m,n \leq N} \frac{a(m)b(n)}{m^{\tau_1} n^{\tau_2}} \int_{\mathbb{R}} \omega(t) \left(\frac{n}{m}\right)^{it} dt.$$

By (3.12), the diagonal terms $m = n$ contribute

$$\sum_{m \leq N} \frac{a(m)b(m)}{m^{\tau_1+\tau_2}} \int_{\mathbb{R}} \omega(t) dt = \widehat{\omega}(0) \sum_{m \leq N} \frac{a(m)b(m)}{m^{\tau_1+\tau_2}}.$$

The remaining terms are of the form $m < n$ and $n < m$. In each of these regions we make the variable changes $n = m + h$ and $m = n + h$ respectively where $h \geq 1$. The off-diagonals

terms ($m \neq n$) thus are

$$\sum_{m,h} \frac{a(m)b(m+h)}{m^{\tau_1}(m+h)^{\tau_2}} \widehat{\omega}\Big(-\frac{\log(\frac{m+h}{m})}{2\pi}\Big) + \sum_{n,h} \frac{b(n)a(n+h)}{n^{\tau_2}(n+h)^{\tau_1}} \widehat{\omega}\Big(\frac{\log(\frac{n+h}{n})}{2\pi}\Big). \tag{3.13}$$

It is clear from this last formula that it will be important to understand the behaviour of correlations sums given by (3.5). For $\widehat{\omega}$ with nice decay properties it follows from Riemann-Stieltjes integration that

$$I_{a,b,\tau_1,\tau_2,\omega} = \widehat{\omega}(0) \sum_{m \leq N} \frac{a(m)b(m)}{m^{\tau_1+\tau_2}} + \sum_{\substack{|h| \leq H \\ h \neq 0}} \int_{|h|T^{1-\varepsilon}}^{N-h} \mathscr{M}'_{a,b;h}(x,h)W(x,h)dx$$
$$+ O(N^{1-(\tau_1+\tau_2)+\max(\vartheta(a,b),\vartheta(b,a))+\varepsilon}), \tag{3.14}$$

where $H = NT^{\varepsilon-1}$ and $W(x,h) = \dfrac{\widehat{\omega}\left(-\frac{\log(\frac{x+h}{x})}{2\pi}\right)}{(x+h)^{\tau_1}x^{\tau_2}}$. This can be proven by following closely the argument of Goldston and Gonek [28]. In the case that $\vartheta = \max(\vartheta(a,b),\vartheta(b,a)) < 1$, this gives an asymptotic formula for $N \ll T^{\frac{1}{1-\vartheta}}$. Thus if $\vartheta = \frac{1}{2} + \varepsilon$, this provides an asymptotic formula for $N \ll T^{2-\varepsilon'}$. A key goal of this chapter is to provide a variant of this formula for a discrete mean value over the zeros of an L-function.

In our work we shall consider certain discrete sums attached to principal L-functions of $\mathrm{GL}(d)$. Let π be an irreducible cupsidal automorphic representation of $\mathrm{GL}(d)$ over $\mathbb{Q}$ with unitary central character. For $\Re(s) > 1$, let

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

is the corresponding L-function. $L(s,\pi)$ has an analytic continuation to the whole complex plane and the non-trivial zeros of $L(s,\pi)$ located in the critical strip $0 < \Re(s) < 1$ shall be denoted ρ_π. We will need to consider the logarithmic derivative

$$-\frac{L'(s,\pi)}{L(s,\pi)} = \sum_{n=1}^{\infty} \frac{\Lambda_\pi(n)}{n^s}. \tag{3.15}$$

We shall consider discrete means of the shape

$$S := S_{\pi,\omega,a,b} = \sum_{\gamma_\pi} \omega(\gamma_\pi) A(\rho_\pi) B(1-\rho_\pi),$$

where $\rho_\pi = \beta_\pi + i\gamma_\pi$ ranges through non tirivial zeros of $L(s,\pi)$ and $\omega(s)$ is a specially chosen weight, holomorphic in a vertical strip. Let T be a large parameter. We begin by considering two other parameters u and Δ which depend on T and satisfy

$$aT \leq u \leq bT \tag{3.16}$$

and

$$\Delta \asymp \frac{T}{\log T}. \tag{3.17}$$

We define an entire weight which depends on u and Δ by

$$\omega(s) := \omega_{\Delta,u}(s) = \Delta^{-1}\pi^{-\frac{1}{2}} e^{(s-(\frac{1}{2}+iu))^2/\Delta^2} \text{ for } s \in \mathbb{C}. \tag{3.18}$$

We think of $\omega(\frac{1}{2}+it)$ as a weight centred at the point $\frac{1}{2}+iu$ and Δ represents the width of of the support of ω. That is, if t is such that $|\frac{t-u}{\Delta}|$ is large then $\omega(\frac{1}{2}+it)$ is very small.

In the case that the length of Dirichlet polynomials is bigger than the length of the integral (i.e., $K \geq T$), then the behaviour of the autocorrelations of the sequence a the correlations of the sequences a and $a*\Lambda$ determine the size of S. Set

$$\mathscr{C}_{a*\Lambda_\pi,b}(x,h) = \sum_{n \leq x} (a*\Lambda_\pi)(n)b(n+h), \tag{3.19}$$

$$\mathscr{C}_{b*\overline{\Lambda_\pi},a}(x,h) = \sum_{n \leq x} (b*\overline{\Lambda_\pi})(n)a(n+h), \tag{3.20}$$

$$\mathscr{C}_{a,b}(x,h) = \sum_{n \leq x} a(n)b(n+h), \tag{3.21}$$

where

$$(a * \Lambda_\pi)(m) = \sum_{jk=m} a(j) \Lambda_\pi(k) = \sum_{\substack{jk=m \\ j \leq M}} a(j) \Lambda_\pi(k), \tag{3.22}$$

by (3.1) and similarly

$$(b * \overline{\Lambda_\pi})(m) = \sum_{jk=m} b(j) \overline{\Lambda_\pi}(k) = \sum_{\substack{jk=m \\ j \leq N}} b(j) \overline{\Lambda_\pi}(k). \tag{3.23}$$

We assume we have expressions of the shape

$$\mathscr{C}_{a*\Lambda_\pi,b;h}(x) = \mathscr{M}_{a*\Lambda_\pi,b;h}(x) + \mathscr{E}_{a*\Lambda_\pi,b;h}(x),$$

$$\mathscr{C}_{b*\overline{\Lambda_\pi},a}(x,h) = \mathscr{M}_{b*\overline{\Lambda_\pi},a;h}(x) + \mathscr{E}_{b*\overline{\Lambda_\pi},a;h}(x), \tag{3.24}$$

$$\mathscr{C}_{a,b;h}(x) = \mathscr{M}_{a,b;h}(x) + \mathscr{E}_{a,b;h}(x),$$

where each of the main terms above are differentiable with respect to x for each h. We set

$$\mathscr{W}(x,h) = \frac{e^{-\frac{\Delta^2 \log^2(1+\frac{h}{x})}{4}}}{\sqrt{x(x+h)}} \left(1 + \frac{h}{x}\right)^{-iT}. \tag{3.25}$$

Theorem 3.1. *Let $n \in \mathbb{N}$ and let $L(s,\pi)$ be the L-function attached to an irreducible cuspidal automorphic representation of $GL(d)$ over $\mathbb{Q}$ with unitary central character. Let A, B be Dirichlet polynomials defined in (3.3). Let $k = \min(M,N)$, $K = \max(M,N)$, and d is the*

52

degree of $L(s, \pi)$. We set $u = T$ in (3.18) and we have that

$$
\sum_{\substack{L(\rho_\pi, \pi) = 0 \\ T/2 < \Im(\rho_\pi) < 2T}} \omega_{\Delta, T}(\rho_\pi) A(\rho_\pi) B(1 - \rho_\pi)
$$

$$
= \frac{d}{2\pi} \big(\log T + O(1) \big) \left(\sum_{|h| \leq \frac{k \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{k} \mathscr{M}'_{a,b;h}(x) \mathscr{W}(x, h) dx + \mathbf{E}_{a,b}(k) \right)
$$

$$
- \sum_{|h| \leq \frac{N \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{N} \mathscr{M}'_{a*\Lambda_\pi, b;h}(x) \mathscr{W}(x, h) dx
$$

$$
- \sum_{|h| \leq \frac{M \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{M} \mathscr{M}'_{b*\overline{\Lambda}_\pi, a;h}(x) \overline{\mathscr{W}(x, h)} dx + \mathbf{E}_{a,b,\Lambda_\pi}(N, M),
$$

where

$$
\mathbf{E}_{a,b,\Lambda_\pi}(N, M) = O\left(\sum_{|h| \leq \frac{N \log T}{\Delta}} \frac{|\mathscr{E}_{a*\Lambda_\pi, b;h}(N)|}{N} + \frac{|\mathscr{E}_{a*\Lambda_\pi, b;h}(\frac{|h|\Delta}{\log T})|}{Th} + \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{N} |\mathscr{E}_{a*\Lambda_\pi, b;h}(x)| x^{-2} dx \right.
$$

$$
\left. + \sum_{|h| \leq \frac{M \log T}{\Delta}} \frac{|\mathscr{E}_{b*\overline{\Lambda}_\pi, a;h}(M)|}{M} + \frac{|\mathscr{E}_{b*\overline{\Lambda}_\pi, a;h}(\frac{|h|\Delta}{\log T})|}{Th} + \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{M} |\mathscr{E}_{b*\overline{\Lambda}_\pi, a;h}(x)| x^{-2} dx \right),
$$

$$
\mathbf{E}_{a,b}(k) = O\left(\sum_{|h| \leq \frac{k \log T}{\Delta}} \frac{|\mathscr{E}_{a,b;h}(k)|}{k} + \frac{|\mathscr{E}_{a,b;h}(\frac{|h|\Delta}{\log T})|}{Th} + \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{k} |\mathscr{E}_{a,b;h}(x)| x^{-2} dx \right).
$$

Remark. The diagonal term (i.e., the term correspondence to $h = 0$) in Theorem 3.1 is

$$
\frac{d}{2\pi} \big(\log T + O(1) \big) \left(\int_{1}^{k} \mathscr{M}'_{a,b;0}(x) x^{-1} dx \right)
$$

$$
- \int_{1}^{N} \mathscr{M}'_{a*\Lambda_\pi, b;0}(x) x^{-1} dx - \int_{1}^{M} \mathscr{M}'_{b*\overline{\Lambda}_\pi, a;0}(x) x^{-1} dx.
$$

In some application the diagonal term forms the main term for S.

Corollary 3.2. *Let A, B be Dirichlet polynomials defined in (3.3). Also assume that we have*

$$
\mathscr{E}_{a*\Lambda_\pi, b;h}(x), \mathscr{E}_{b*\overline{\Lambda}_\pi, a;h}(x), \mathscr{E}_{a,b;h}(x) \ll x^\sigma,
$$

where $0 \leq \sigma < 1$. Then

$$\sum_{\substack{L(\rho_\pi,\pi)=0 \\ T/2 < \Im(\rho_\pi) < 2T}} \omega_{\Delta,T}(\rho_\pi) A(\rho_\pi) B(1-\rho_\pi)$$

$$= \frac{d}{2\pi} \left(\log T + O(1) \right) \left(\sum_{|h| \leq \frac{k \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{k} \mathscr{M}'_{a,b;h}(x) \mathscr{W}(x,h) dx \right)$$

$$- \sum_{|h| \leq \frac{N \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{N} \mathscr{M}'_{a*\Lambda_\pi,b;h}(x) \mathscr{W}(x,h) dx$$

$$- \sum_{|h| \leq \frac{M \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{M} \mathscr{M}'_{b*\overline{\Lambda}_\pi,a;h}(x) \overline{\mathscr{W}(x,h)} dx + O\left(K^\sigma T^{-1} \right).$$

Gaps between the zeros of the Riemann zeta function. We now discuss how our discrete mean value theorems may have applications to the gaps between the zeros of the Riemann zeta function. Assume the Riemann hypothesis and let $\frac{1}{2} + i\gamma_n$ denote the zeros of Riemann zeta function such that

$$0 < \gamma_1 < \gamma_2 < \cdots \leq \gamma_n \leq \gamma_{n+1} \leq \cdots.$$

It follows from Riemann's zero counting formula for $N(T)$ that $\gamma_n \sim \frac{2\pi n}{\log n}$. For this reason, it is useful to define the scaled ordinates $\widehat{\gamma}_n = \frac{\log \gamma_n}{2\pi} \gamma_n$. On average, we have that $\widehat{\gamma}_{n+1} - \widehat{\gamma}_n \sim 1$. In [57], Montgomery studied the pair correlation of the Riemann zeta function, namely the distribution of $\widehat{\gamma}_m - \widehat{\gamma}_n$. Based on his work he made the following conjecture.

Small Gaps Conjecture. We have that

$$\mu = \liminf_{n \to \infty} (\widehat{\gamma}_{n+1} - \widehat{\gamma}_n) = 0. \tag{3.26}$$

From his work on pair correlation he was able to deduce $\mu < 0.68$. Later, by a different method, Montgomery and Odlyzko [58] showed that $\mu < 0.5179$. Conrey, Ghosh, and Gonek [12] slightly improved this to $\mu < 0.5172$. Bui, Milinovich, and Ng [8] reduced this

to $\mu < 0.5155$. This was later improved by Feng and Wu [25]. These arguments are based on ideas of Montgomery, Odlyzko [58] and Mueller [63] which we now describe. Let φ be a non-negative function defined on $[T/2, 2T]$ where T is a large parameter. Define

$$Q_{\varphi}(c,T) := \frac{\displaystyle\int_{-\frac{c\pi}{\log T}}^{\frac{c\pi}{\log T}} \sum_{T/2 \leq \gamma \leq 2T} \varphi(\gamma + \alpha) d\alpha}{\displaystyle\int_{T/2}^{2T} \varphi(t) dt}. \tag{3.27}$$

If it can be shown that there exists a function φ and a parameter c such that $Q_{\varphi}(c,T) > 1$ for all sufficiently large T, then it follows that $\mu \leq c$.

Conrey, Ghosh, and Gonek made the choice

$$\varphi(t) = \Big| \sum_{n \leq T(\log T)^{-2}} \frac{a(n)}{n^{it}} \Big|^2, \tag{3.28}$$

where $a(n)$ is an arbitrary sequence satisfying $|a(n)| \ll n^{\varepsilon}$. They showed that for this choice

$$Q_{\varphi}(c,T) = c - \frac{\frac{2}{\pi}\Re\Big(\sum_{nk \leq K} \frac{\Lambda(n)a(k)\overline{a(nk)}\sin\left(\pi c \frac{\log n}{\log T}\right)}{\sqrt{n}\log n}\Big)}{\sum_{k \leq K}|a(k)|^2} + o_{T \to \infty}(1).$$

Furthermore, they proved that if $c < 0.5$, then $Q_{\varphi}(c,T) < 1$. Interestingly, Goldston, in an unpublished work has shown that if $c < 0.50001$, then $Q_{\varphi}(c,T) < 1$. Thus this choice cannot be used to show $\mu \leq 0.50001$. In order to make the quotient $Q_{\varphi}(c,T)$ large, one may choose coefficients of the shape

$$a(n) = \mu_r(n)n^{-\frac{1}{2}}f\Big(\frac{\log n}{\log N}\Big) \text{ for } n \leq N,$$

where $N = T(\log T)^{-2}$, $\zeta(s)^{-r} = \sum_{n=1}^{\infty}\mu_r(n)n^{-s}$ for $r \geq 1$, and f is a smooth function. For

55

this choice

$$\varphi(t) = \Big| \sum_{n \leq T(\log T)^{-2}} \frac{\mu_r(n)}{n^{\frac{1}{2}+it}} f\Big(\frac{\log n}{\log N}\Big) \Big|^2.$$

may be viewed as some sort of approximation to $|\zeta(\frac{1}{2}+it)|^{-2r}$ and thus φ is large at the zeros of $\zeta(s)$. In light of Goldston's work, we shall consider Dirichlet polynomials with length greater than T. Let

$$\varphi_1(t) = \omega(\tfrac{1}{2}+it) \Big| \sum_{n \leq K} \frac{a(n)}{n^{it}} \Big|^2 \tag{3.29}$$

where ω is defined by (3.18), $K = T^\vartheta$ and $\vartheta \geq 1$. The weight $\omega(\frac{1}{2}+it)$ is included for technical reasons; it is used to simplify the evaluation of various contour integrals. We shall evaluate (3.27) with the choice φ_1.

Corollary 3.3. *Let A be the Dirichlet polynomial defined in (3.3) and for $\alpha \in \mathbb{R}$ set*

$$a_\alpha(n) := a(n)n^{i\alpha}. \tag{3.30}$$

We assume the following regarding the error terms in Theorem 3.1:
$\mathbf{E}_{a_\alpha, \overline{a_\alpha}, \Lambda_\pi}(K, K) = o(N)$ *and* $\mathbf{E}_{a_\alpha, \overline{a_\alpha}}(K) = o(D)$, *where*

$$D = \sum_{|h| \leq \frac{K \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{K} \mathcal{M}'_{a,\overline{a};h}(x) \mathcal{W}(x,h) dx,$$

$$N = cD - 2\Re\Bigg(\sum_{|h| \leq \frac{K \log T}{\Delta}} \int_{-\frac{c\pi}{\log T}}^{\frac{c\pi}{\log T}} \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{K} \mathcal{M}'_{a_\alpha * \Lambda_\pi, \overline{a}_{-\alpha};h}(x) \mathcal{W}(x,h) dx \, d\alpha \Bigg).$$

Therefore we have

$$Q_{\varphi_1}(c, T) = \frac{N}{D} + o\Big(\frac{N}{D} + 1\Big). \tag{3.31}$$

We can re-write (3.31) *as*

$$Q_{\varphi_1}(c,T) = \big(1+o(1)\big)\times$$

$$\left(c - \frac{\int_{-\frac{c\pi}{\log T}}^{\frac{c\pi}{\log T}} 2\Re\left(\sum_{|h|\leq \frac{K\log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T},1)}^{K} \mathscr{M}'_{a_\alpha*\Lambda_\pi,\bar{a}_{-\alpha};h}(x)\mathscr{W}(x,h)dx\right)d\alpha}{\sum_{|h|\leq \frac{K\log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T},1)}^{K} \mathscr{M}'_{a,\bar{a};h}(x)\mathscr{W}(x,h)dx}\right).$$

In the case of $L(s,\pi) = \zeta(s)$, we would like to choose coefficients $a(n)$ so that $\varphi_1(t) > 1$ for some $c < \frac{1}{2}$. Unfortunately, we currently do not know how to find such $a(n)$. The above result tells us in order to do this, we need to know how calculate the correlations $\mathscr{C}_{a,a;h}(x)$ and $\mathscr{C}_{a*\Lambda_\pi,a;h}(x)$. An appropriate choice for $a(n)$ is $a(n) = \lambda(n) := (-1)^{\Omega(n)}$, the Liouville function, where $\Omega(n)$ is the total number of prime factors of n. This leads us to correlation of $\lambda(n)$.

Chowla's famous conjecture, Problem 57 in [11], addresses this.

Chowla's conjecture. Let $f(x)$ be an arbitrary polynomial with integer coefficients, which is not of the form $cg(x)^2$ where c is an integer and $g(x)$ is a polynomial with integer coefficients. Then

$$\sum_{n\leq x} \lambda(f(n)) = o(x).$$

We now state three related conjectures that we will be used in our result on the gaps between the zeros of the Riemann zeta function.

Shfited convolution sums of the Liouville and von Mangoldt functions.

$LV(\eta_0,\sigma_0,\delta_0)$: For the triple $(\eta_0,\sigma_0,\delta_0)$ of positive numbers, if x is large,

$1 \leq a \leq x^{\eta_0}, 1 \leq b \leq x^{\sigma_0}$, then uniformly   (3.32)

$$\sum_{n<x} (\lambda_\alpha * \Lambda)(n)\lambda_{-\alpha}(an+b) \ll x^{\delta_0}$$

Chowla's Conjecture (strong form).

$Ch_1(\eta_1, \sigma_1, \delta_1)$: For the triple $(\eta_1, \sigma_1, \delta_1)$ of positive numbers, if x is large,

$$1 \leq a \leq x^{\eta_1}, 1 \leq b \leq x^{\sigma_1}, \text{ then uniformly} \tag{3.33}$$

$$\sum_{n \leq x} \lambda(n) \lambda(an + b) \ll x^{\delta_1}.$$

Chowla's conjecture (for prime values).

$Ch_2(\eta_2, \sigma_2, \delta_2)$: For the triple $(\eta_2, \sigma_2, \delta_2)$ of positive numbers, if x is large,

$$1 \leq a \leq x^{\eta_1}, 1 \leq b \leq x^{\sigma_2}, \text{ then uniformly} \tag{3.34}$$

$$\sum_{p \leq x} \lambda(ap + b) \ll x^{\delta_2}.$$

Later we discuss the relationship between the above conjectures.

Corollary 3.4. *Assume the Riemann hypothesis and the statements* $LV(0, \frac{1}{12}, \frac{92}{100})$ *and* $Ch_1(0, \frac{1}{12}, \frac{92}{100})$ *hold. Then we have that*

$$\mu < 0.4999.$$

In other words the gaps between consecutive zeros of the Riemann zeta function are infinitely often smaller than one half of the average gap.

Remark 3.5. In the discussion section we will show that instead of $LV(0, \frac{1}{12}, \frac{92}{100})$ and $Ch_1(0, \frac{1}{12}, \frac{92}{100})$ we can assume $Ch_1(1, \frac{1}{12}, \frac{84}{100})$ and $Ch_2(1, \frac{1}{12}, \frac{84}{100})$ and same result as above will hold.

3.2   Properties of principal *L*-functions

Let π be an irreducible cuspidal automorphic representation of $GL(d)$ over $\mathbb{Q}$ with unitary central character. Attached to π is its *L*-function $L(s, \pi)$. These functions were defined by Godement and Jacquet in [27]. For $\Re(s) > 1$, $L(s, \pi)$ has an Euler product of the form

$$L(s, \pi) = \prod_{p} \prod_{j=1}^{m} \left(1 - \frac{\alpha_j(p)}{p^s}\right)^{-1}. \tag{3.35}$$

58

It is known that $L(s,\pi)$ is either the Riemann zeta function or is an entire function of order 1. Its completed L-function is

$$\Phi(s,\pi) = N^{s/2}\gamma(s,\pi)L(s,\pi)$$

where N is a natural number and the gamma factor $\gamma(s,\pi)$ is defined by

$$\gamma(s,\pi) = \prod_{j=1}^{m}\Gamma_{\mathbb{R}}(s+\mu_j) \tag{3.36}$$

where $m \in \mathbb{N}$, μ_j's are complex numbers, and $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$. Using the above notation we have the functional equation:

$$\Phi(s,\pi) = \varepsilon_\pi\overline{\Phi}(1-s,\pi). \tag{3.37}$$

where $\varepsilon_\pi \in \mathbb{C}$ with $|\varepsilon_\pi| = 1$, and $\overline{\Phi}(s,\pi) = \overline{\Phi(\bar{s},\pi)}$.

3.3 The weight function

The weight. For $c \in \mathbb{R}$, we write

$$\int_{(c)} f(s)ds = \int_{c-i\infty}^{c+i\infty} f(s)ds.$$

In the rest of this chapter we will use of the following lemma:

Lemma 3.6. *Let $c \in \mathbb{R}$ and $x > 0$. Then*

$$\frac{1}{2\pi i}\int_{(c)}\omega(s)x^s ds = \frac{1}{2\pi}x^{\frac{1}{2}+iu}e^{-\frac{\Delta^2\log^2 x}{4}}, \tag{3.38}$$

$$\frac{1}{2\pi i}\int_{(c)}\omega(1-s)x^s ds = \frac{1}{2\pi}x^{\frac{1}{2}-iu}e^{-\frac{\Delta^2\log^2 x}{4}}, \tag{3.39}$$

$$\int_{-\infty}^{\infty}\omega(\tfrac{1}{2}+it)dt = 1. \tag{3.40}$$

Proof. On page 5 of [5] it is proven that

$$\int_{(c)} e^{(s-s_0)^2/\Delta^2} x^{-s} ds = i\Delta\sqrt{\pi} x^{-s_0} \exp(-\frac{\Delta^2 \log^2 x}{4}).$$

Therefore (3.38) and (3.39) follows from the above by choosing $s_0 = \frac{1}{2} + iu$. Lastly, (3.40) is given by

$$\int_{-\infty}^{\infty} \omega(\tfrac{1}{2} + it) dt = \Delta^{-1} \pi^{-\frac{1}{2}} \int_{-\infty}^{\infty} e^{-(t-u)^2/\Delta^2} dt = 1. \tag{3.41}$$

$\square$

Now we give a proof of our theorem.

Proof of Theorem 3.1. Consider

$$S := \sum_{L(\rho_\pi, \pi)=0} \omega(\rho_\pi) A(\rho_\pi) B(1 - \rho_\pi),$$

$$I_R = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \omega(s) A(s) B(1-s) \frac{L'}{L}(s, \pi) ds \tag{3.42}$$

and

$$I_L = \frac{1}{2\pi i} \int_{1-c-i\infty}^{1-c+i\infty} \omega(s) A(s) B(1-s) \frac{L'}{L}(s, \pi) ds \tag{3.43}$$

where $1 < c < 2$. Moving the contour in I_R to the left from $\Re(s) = c$ to $\Re(s) = 1 - c$ and applying the residue theorem establish

$$S = I_R - I_L. \tag{3.44}$$

We simplify I_L. The functional equation may be written in unsymmetrical form as

$$L(s, \pi) = \chi_\pi(s)\overline{L(1 - \bar{s}, \pi)}$$

60

where

$$\chi_\pi(s) = \varepsilon_\pi N^{\frac{1}{2}-s} \overline{\gamma(1-\bar{s},\pi)} \gamma(s,\pi)^{-1}.$$

Taking logarithmic derivatives, we have

$$\frac{L'}{L}(1-c+it,\pi) = \frac{\chi'_\pi}{\chi_\pi}(1-c+it) - \frac{\overline{L'}}{L}(c-it,\pi), \qquad (3.45)$$

where

$$\frac{\overline{L'}}{L}(s,\pi) := \sum_{n=1}^{\infty} \frac{\overline{\Lambda_\pi(n)}}{n^s}$$

and

$$\frac{\chi'_\pi}{\chi_\pi}(s) = -\log N - \frac{\overline{\gamma'}}{\gamma}(1-\bar{s},\pi) - \frac{\gamma'}{\gamma}(s,\pi).$$

Thus $I_L = J_1 - J_2$, where

$$J_1 = \frac{1}{2\pi i} \int_{(1-c)} \omega(s)A(s)B(1-s)\frac{\chi'_\pi}{\chi_\pi}(s)ds, \qquad (3.46)$$

$$J_2 = \frac{1}{2\pi i} \int_{(1-c)} \omega(s)A(s)B(1-s)\frac{\overline{L'}}{L}(1-s,\pi)ds. \qquad (3.47)$$

We now have

$$S = I_R - J_1 + J_2. \qquad (3.48)$$

Thus the evaluation of S has been reduced to that of I_R, J_1, and J_2. We further simplify J_2. By the variable change $s \to 1-s$ it follows that

$$J_2 = \frac{1}{2\pi i} \int_{(c)} \omega(1-s)A(1-s)B(s)\frac{\overline{L'}}{L}(s,\pi)ds. \qquad (3.49)$$

Observe that this now has a very similar form to (3.42). Thus I_R and J_2 may be treated similarly. By the absolute convergence of the Dirichlet series in (3.42) and (3.49), we

expand out the above integrate termwise to obtain

$$I_R = -\frac{1}{2\pi i} \sum_{m=1}^{\infty} \sum_{n \leq N} \frac{(a * \Lambda_\pi)(m)b(n)}{n} \int_{(c)} \omega(s) \left(\frac{n}{m}\right)^s ds,$$

$$J_2 = -\frac{1}{2\pi i} \sum_{m=1}^{\infty} \sum_{n \leq M} \frac{(b * \overline{\Lambda_\pi})(m)a(n)}{n} \int_{(c)} \omega(1-s) \left(\frac{n}{m}\right)^s ds.$$

where $(a * \Lambda_\pi)(m)$ and $(b * \overline{\Lambda_\pi})(m)$ are given by (3.22) and (3.23).

3.3.1 Evaluation of I_R, J_2

We now proceed to evaluate I_R and J_2. By Lemma 3.6 with $x = n/m$

$$I_R = -\frac{1}{2\pi} \sum_{m=1}^{\infty} \frac{(a * \Lambda_\pi)(m)}{\sqrt{m}} \sum_{n \leq N} \frac{b(n)}{\sqrt{n}} \left(\frac{n}{m}\right)^{iu} e^{-\frac{\Delta^2 \log^2(\frac{n}{m})}{4}}. \tag{3.50}$$

and similarly

$$J_2 = -\frac{1}{2\pi} \sum_{m=1}^{\infty} \frac{(b * \overline{\Lambda_\pi})(m)}{\sqrt{m}} \sum_{n \leq M} \frac{a(n)}{\sqrt{n}} \left(\frac{n}{m}\right)^{-iu} e^{-\frac{\Delta^2 \log^2(\frac{n}{m})}{4}}. \tag{3.51}$$

We remove n and m such that $\Delta |\log(\frac{n}{m})| \geq \log T$ to obtain a bound of $O(e^{-c(\log T)^2})$. We set $m = n + h$ and $u = T$ and we have I_R equals

$$\sum_{|h| \leq \frac{N \log T}{\Delta}} \sum_{\max(\frac{|h|\Delta}{\log T}, 1) \leq n \leq N} (a * \Lambda_\pi)(n+h)b(n)\mathscr{W}(n,h) + O(e^{-c(\log T)^2}). \tag{3.52}$$

Recall that $\mathscr{W}(n,h) = \frac{e^{-\frac{\Delta^2 \log^2(1+\frac{h}{n})}{4}}}{\sqrt{n(n+h)}} \left(1 + \frac{h}{n}\right)^{-iT}$. Similarly we have

$$J_2 = \sum_{|h| \leq \frac{M \log T}{\Delta}} \sum_{\max(\frac{|h|\Delta}{\log T}, 1) \leq n \leq M} (b * \overline{\Lambda_\pi})(n+h)a(n)\overline{\mathscr{W}(n,h)} + O(e^{-c(\log T)^2}). \tag{3.53}$$

By the Riemann-Stieltjes integration and (3.19) we have that

$$
I_R = \sum_{|h| \le \frac{N \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{N} \left(\mathscr{M}'_{a*\Lambda_\pi, b; h}(x) \mathscr{W}(x, h) dx + \mathscr{W}(x, h) d\mathscr{E}_{a*\Lambda_\pi, b; h}(x) \right) dx
$$
$$
+ O(e^{-c(\log T)^2}).
$$

Similarly, by employing (3.20) we have

$$
J_2 = \sum_{|h| \le \frac{M \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{M} \left(\mathscr{M}'_{b*\overline{\Lambda}_\pi, a; h}(x) \overline{\mathscr{W}(x, h)} dx + \overline{\mathscr{W}(x, h)} d\mathscr{E}_{b*\overline{\Lambda}_\pi, a; h}(x) \right) dx
$$
$$
+ O(e^{-c(\log T)^2}).
$$

An integration by parts yields

$$
\sum_{|h| \le \frac{N \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{N} \mathscr{W}(x, h) d\mathscr{E}_{a*\Lambda_\pi, b; h}(x)
$$
$$
= \sum_{|h| \le \frac{N \log T}{\Delta}} \left(\mathscr{W}(x, h) \mathscr{E}_{a*\Lambda_\pi, b; h}(x) \Big]_{\max(\frac{|h|\Delta}{\log T}, 1)}^{N} - \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{N} \mathscr{E}_{a*\Lambda_\pi, b; h}(x) d\mathscr{W}(x, h) dx \right).
$$
$$
(3.54)
$$

Now by considering the fact that

$$
\frac{\partial}{\partial x} \mathscr{W}(x, h) \ll x^{-2},
$$

we have that (3.54) contribute

$$
O\left(\sum_{|h| \le \frac{N \log T}{\Delta}} \frac{|\mathscr{E}_{a*\Lambda_\pi, b; h}(N)|}{N} + \frac{|\mathscr{E}_{a*\Lambda_\pi, b; h}(\frac{|h|\Delta}{\log T})|}{Th} + \int_{\max(\frac{|h|\Delta}{\log T}, 1)}^{N} |\mathscr{E}_{a*\Lambda_\pi, b; h}(x)| x^{-2} dx \right), \quad (3.55)
$$

to the error term in Theorem 3.1.

3.3.2 Evaluation of J_1

Finally, we must evaluate J_1. Observe that the poles of $\chi_\pi(s)$ lie in the set

$$\bigcup_{j=1}^{m} \{-\mu_j - k \mid k \in \mathbb{Z}_{\geq 0}\}.$$

Label these poles as c_j for $1 \leq j \leq m$. Moving the contour to the right to the line $\Re(s) = 1/2$ yields

$$J_1 = -\frac{1}{2\pi i} \int_{(\frac{1}{2})} \omega(s)A(s)B(1-s)\frac{\chi_\pi'}{\chi_\pi}(s)ds + O\Big(\sum_{\text{poles } c_j} \omega(c_j)A(c_j)B(1-c_j)\Big),$$

where the O-term is the contribution from the pole at $s = 0$ and it may be shown that this is $O(e^{-c\log^2 T})$ for some $c > 0$. The integral is

$$-\frac{1}{2\pi} \int_{-\infty}^{\infty} \omega(\tfrac{1}{2}+it)A(\tfrac{1}{2}+it)B(\tfrac{1}{2}-it)\frac{\chi_\pi'}{\chi_\pi}(\tfrac{1}{2}+it)dt$$

$$= -\frac{1}{2\pi} \int_{-\infty}^{\infty} \frac{1}{\Delta\sqrt{\pi}}e^{-\frac{(t-u)^2}{\Delta^2}}A(\tfrac{1}{2}+it)B(\tfrac{1}{2}-it)\frac{\chi_\pi'}{\chi_\pi}(\tfrac{1}{2}+it)dt$$

$$= -\frac{1}{2\pi} \int_{T_1}^{T_2} \frac{1}{\Delta\sqrt{\pi}}e^{-\frac{(t-u)^2}{\Delta^2}}A(\tfrac{1}{2}+it)B(\tfrac{1}{2}-it)\frac{\chi_\pi'}{\chi_\pi}(\tfrac{1}{2}+it)dt + O(e^{-0.99(\log T)^2})$$

where $T_1 = T - \Delta\log T$ and $T_2 = T + \Delta\log T$. Denote the last integral in the above as J_1'.

Let

$$g(t) = -\frac{\chi_\pi'}{\chi_\pi}(\tfrac{1}{2}+it) \text{ and } \phi(t) = \frac{1}{\Delta\sqrt{\pi}}e^{-\frac{(t-T)^2}{\Delta^2}}A(\tfrac{1}{2}+it)B(\tfrac{1}{2}-it).$$

Then

$$J_1' = \frac{1}{2\pi} \int_{T_1}^{T_2} \phi(t)g(t)dt. \tag{3.56}$$

We now determine an asymptotic expansion for $g(t)$. We have

$$g(t) = \log N + \frac{\gamma'}{\gamma}(\tfrac{1}{2}+it,\pi) + \frac{\gamma'}{\gamma}(\tfrac{1}{2}+it,\pi)$$

$$= \log N + 2\Re\frac{\gamma'}{\gamma}(\tfrac{1}{2}+it,\pi)$$

$$= \log N + 2\Big(\sum_{j=1}^{d} \Re\frac{\Gamma'_{\mathbb{R}}}{\Gamma_{\mathbb{R}}}(\tfrac{1}{2}+it-\mu_j)\Big).$$

Observe that

$$\frac{\Gamma'_{\mathbb{R}}}{\Gamma_{\mathbb{R}}}(s) = -\frac{\log\pi}{2} + \frac{1}{2}\frac{\Gamma'}{\Gamma}(\tfrac{s}{2})$$

and thus

$$g(t) = \log N - d\log\pi + \sum_{j=1}^{d}\Re\frac{\Gamma'}{\Gamma}(\tfrac{1}{4}-\tfrac{\mu_j}{2}+i\tfrac{t}{2}). \tag{3.57}$$

Note that for $\delta > 0$ fixed and $|\arg(z)| \leq \pi - \delta$,

$$\frac{\Gamma'}{\Gamma}(z) = \log z - \frac{1}{2z} + O_\delta(|z|^{-2}).$$

Taking real parts, we obtain in the same region

$$\Re\frac{\Gamma'}{\Gamma}(z) = \log|z| + O_\delta(|z|^{-1}).$$

Now we can check that

$$\log|\tfrac{1}{4}-\tfrac{\mu_j}{2}+i\tfrac{t}{2}| = \log|t| + c + O(|t|^{-1}).$$

Inserting this is (3.57) yields

$$g(t) = \log N - d\log\pi + d(\log(|t|)+c) + O(dt^{-1}).$$

65

Integrating by parts yields

$$J_1' = \frac{1}{2\pi} \int_{T_1}^{T_2} \phi(t)g(t)dt$$

$$= \frac{1}{2\pi} \left(g(t) \int_{T_1}^{t} \phi(x)dx \Big|_{T_1}^{T_2} - \int_{T_1}^{T_2} g'(t) \left(\int_{T_1}^{t} \phi(x)dx \right) dt \right).$$

Note that

$$g(t) = d\log t + c_0 + c_1 t^{-1} + O(t^{-2}),$$

$$g'(t) = dt^{-1} + O(t^{-2})$$

and

$$\int_{T_1}^{T_2} \phi(t)dt = \int_{-\infty}^{\infty} \phi(t)dt + O(e^{-0.99(\log u)^2}).$$

Using these estimates

$$J_1' = \frac{1}{2\pi} \left(d(\log T_2 + O(1)) \int_{-\infty}^{\infty} \phi(t)dt + O\left(\int_{T_1}^{T_2} t^{-1} \Big| \int_{T_1}^{t} \phi(x)dx \Big| dt \right) \right)$$

The second error term is

$$\ll \frac{T_2 - T_1}{T_2} \int_{T_1}^{T_2} \phi(t)dt \ll \frac{\Delta \log T}{T_2} \int_{-\infty}^{\infty} \phi(t)dt. \tag{3.58}$$

Also

$$\log T_2 = \log T + \log(\frac{T_2}{T}) = \log T + \log\left(1 + \frac{\Delta \log T}{T} \right) = \log T + O\left(\frac{\Delta \log T}{T} \right)$$

Putting everything together

$$J_1' = \frac{1}{2\pi} \left((d\log T + O(1 + \frac{\Delta \log T}{T})) \int_{-\infty}^{\infty} \phi(t)dt \right.$$

$$\int_{-\infty}^{\infty} \phi(t)dt = \int_{-\infty}^{\infty} e^{-\frac{(t-T)^2}{\Delta^2}} A(\tfrac{1}{2}+it)B(\tfrac{1}{2}-it)dt$$

and thus

$$J_1 = \frac{1}{2\pi}\Big(d(\log T + O(1+\frac{\Delta \log T}{T}))\Big)\frac{1}{\Delta\sqrt{\pi}}\int_{-\infty}^{\infty} e^{-\frac{(t-T)^2}{\Delta^2}} A(\tfrac{1}{2}+it)B(\tfrac{1}{2}-it)dt$$

To finish the proof we apply Lemma 3.7 to the above integral. $\square$

Proof of Corollary 3.2. By Using the bound $|\mathcal{E}_{a*\Lambda_\pi,b;h}(x,h)| \ll x^\sigma$ in (3.55) we obtain an error term $O(N^\sigma/T)$. We have a similar calculation for J_2. $\square$

Lemma 3.7. *Let A,B be Dirichlet polynomials defined in (3.3). Let*

$$I = \int_{\mathbb{R}} \omega(t)A(\tfrac{1}{2}+it)B(\tfrac{1}{2}-it)dt. \tag{3.59}$$

Then we have that

$$I = \sum_{|h|\le \frac{k\log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T},1)}^{k} \mathcal{M}'_{a,b;h}(x)\mathcal{W}(x,h)dx + \mathbf{E}_{a,b}(k), \tag{3.60}$$

where

$$\mathbf{E}_{a,b}(k) = \Bigg(\sum_{|h|\le \frac{k\log T}{\Delta}} \frac{|\mathcal{E}_{a,b;h}(k)|}{k} + \frac{|\mathcal{E}_{a,b;h}(\frac{|h|\Delta}{\log T})|}{Th} + \int_{\max(\frac{|h|\Delta}{\log T},1)}^{k} |\mathcal{E}_{a,b;h}(x)|x^{-2}dx\Bigg).$$

Proof. This follows similar argument to our estimation of I_R and J_2. The main difference is here we only need to consider the shifted convolutions of $a(n)$ and $b(n)$.

$\square$

3.4 Small gaps between the zeros of the zeta function

In this section we establish Corollary 3.3 which provides a formula for $Q_{\varphi_1}(c,T)$.

Proof of corollary 3.3. Observe that

$$Q_{\varphi_1}(c,T) = \frac{\int_{-\frac{c\pi}{\log T}}^{\frac{c\pi}{\log T}} \sum_{T/2 \leq \gamma \leq 2T} \omega(\frac{1}{2} + i(\gamma + \alpha))|A(\frac{1}{2} + i(\gamma + \alpha))|^2 d\alpha}{\int_{T/2}^{2T} \omega(\frac{1}{2} + it)|A(\frac{1}{2} + it)|^2 dt} \tag{3.61}$$

To prove the corollary we take $\phi(t) = |A(\frac{1}{2} + it)|^2 \omega(\frac{1}{2} + it)$, and apply Theorem 3.1 by considering $a_\alpha(n) = a(n)n^{i\alpha}$ in place of $a(n)$ and $\bar{a}_{-\alpha}(n) = \overline{a(n)}n^{-i\alpha}$ in place of $b(n)$. Note that since $\omega(\frac{1}{2} + it)$ is positive therefore by the Mean Value Theorem there exist $\tilde{t} \in [t, t + \alpha]$ such that

$$|\omega(\tfrac{1}{2} + i(t + \alpha)) - |\omega(\tfrac{1}{2} + it)| < T^{-1+\varepsilon}\omega(\tfrac{1}{2} + i\tilde{t}) \ll T^{-1+\varepsilon}\omega(\tfrac{1}{2} + it).$$

Thefore we can apply Theorem 3.1 to get

$$Q(c,T) = \frac{N}{D} + \mathbf{E} \tag{3.62}$$

where

$$N = \int_{-\frac{c\pi}{\log T}}^{\frac{c\pi}{\log T}} \left(\frac{\log T}{2\pi} + O(1)\right) \sum_{|h| \leq \frac{K\log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T},1)}^{K} \mathcal{M}'_{a,\bar{a};h}(x)\mathcal{W}(x,h)\left(\frac{x}{x+h}\right)^{i\alpha} dx d\alpha$$

$$- 2\Re\left(\sum_{|h| \leq \frac{K\log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T},1)}^{K} \mathcal{M}'_{a_\alpha * \Lambda_\pi, \bar{a}_{-\alpha};h}(x)\mathcal{W}(x,h)dx\right)d\alpha$$

and

$$D = \sum_{|h| \leq \frac{K\log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T},1)}^{K} \mathcal{M}'_{a,\bar{a};h}(x)\mathcal{W}(x,h)dx.$$

We integrate with respect to α in the first integrand of N and we have

$$\int_{-\frac{c\pi}{\log T}}^{\frac{c\pi}{\log T}} \left(\frac{\log T}{2\pi} + O(1)\right) \sum_{|h| \leq \frac{K \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T},1)}^{K} \mathscr{M}'_{a,\overline{a};h}(x) \mathscr{W}(x,h) \left(\frac{x}{x+h}\right)^{i\alpha} dx d\alpha$$

$$= c + O(\tfrac{1}{\log T})) \sum_{|h| \leq \frac{K \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T},1)}^{K} \mathscr{M}'_{a,\overline{a};h}(x) \mathscr{W}(x,h) dx$$

$$+ O\left(\frac{1}{T} \sum_{|h| \leq \frac{K \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T},1)}^{K} \mathscr{M}'_{a,\overline{a};h}(x) \mathscr{W}(x,h) dx\right)$$

Therefore we have

$$\frac{N}{D} = c - \frac{\int_{-\frac{c\pi}{\log T}}^{\frac{c\pi}{\log T}} 2\Re\left(\sum_{|h| \leq \frac{K \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T},1)}^{K} \mathscr{M}'_{a_\alpha * \Lambda_\pi, \overline{a}_{-\alpha};h}(x) \mathscr{W}(x,h) dx\right) d\alpha}{\sum_{|h| \leq \frac{K \log T}{\Delta}} \int_{\max(\frac{|h|\Delta}{\log T},1)}^{K} \mathscr{M}'_{a,\overline{a};h}(x) \mathscr{W}(x,h) dx} + O(\tfrac{1}{\log T}).$$

For the error term $\mathbf{E}$ we have

$$\mathbf{E} = \frac{\mathbf{E}_{a_\alpha, \overline{a_\alpha}, \Lambda_\pi}(K,K) D + \mathbf{E}_{a_\alpha, \overline{a_\alpha}}(K) D - \mathbf{E}_{a_\alpha, \overline{a}}(K) N}{D(D + \mathbf{E}_{a_\alpha, \overline{a_\alpha}}(K))} \tag{3.63}$$

Here we use the assumption that $\mathbf{E}_{a_\alpha, \overline{a_\alpha}, \Lambda_\pi}(K,K) = o(N)$ and $\mathbf{E}_{a_\alpha, \overline{a_\alpha}}(K) = o(D)$ and therefore we have

$$\mathbf{E} = o\left(\left|\frac{N}{D}\right| + 1\right). \tag{3.64}$$

This shows that $Q(c,T) \sim \dfrac{N}{D}$, as $T \longrightarrow \infty$. $\qquad\square$

To prove Corollary 3.4 we need to apply Corollary 3.3 to

$$A(s) = \sum_{n \leq K} \frac{\lambda(n) n^{i\alpha}}{n^s}. \tag{3.65}$$

Note that we will take K to be much larger than T and therefore we will have off diagonal contribution. However, we will show that that the off-diagonal contribution is negligible. In order to use Corollary 3.3 need to show $\mathbf{E}_{\lambda, \lambda, \Lambda}(K,K) = o(N)$ and $\mathbf{E}_{\lambda, \lambda}(K) = o(D)$. By

assuming $LV\left(0,\frac{1}{2},\delta\right)$, for $h \neq 0$ we have

$$\sum_{n \leq x} (\lambda_{-\alpha} * \Lambda)(n)\lambda_\alpha(n+h) \ll x^\delta. \tag{3.66}$$

This shows that for $h \neq 0$, $\mathcal{M}_{\lambda_{-\alpha}*\Lambda,\lambda_\alpha;h}(x) = 0$ and $\mathcal{E}_{\lambda_{-\alpha}*\Lambda,\lambda_\alpha;h}(x,h) = O(x^\delta)$. We also have $\mathcal{E}_{\lambda_{-\alpha},\lambda_\alpha;h} \ll x^{\delta_1}$ by the strong form of Chowla's conjecture with $a = 1$, $Ch_1\left(0,\frac{1}{2},\delta_1\right)$. This shows that we can take $K = T^{2/(1+\delta)-\varepsilon}$ and have $\mathbf{E}_{\lambda,\lambda,\Lambda}(K,K) = o(N)$ and $\mathbf{E}_{\lambda,\lambda}(K) = o(D)$. Consequently we can apply Corollary 3.3 to (3.65)

Proof of Corollary 3.4. Let c be positive such that $c = O(1)$ and let $K = T^\theta$. We apply Corollary 3.3 to (3.65) and we have

$$Q_{\varphi_1}(c,T) \sim c - \frac{\int_{-\frac{c\pi}{\log T}}^{\frac{c\pi}{\log T}} 2\Re\left(\int_1^K \mathcal{M}'_{\lambda_\alpha*\Lambda,\lambda_{-\alpha}}(x)W(x,0)dx \right) d\alpha}{\int_1^K \mathcal{M}'_{\lambda,\lambda}(x)W(x,0)dx} \tag{3.67}$$

We have that $W(x,0) = x^{-1}$ and therefore we can rewrite the integrals in the above as the corresponding summations and therefore we have

$$Q_{\varphi_1}(c,T) \sim \left(c - \frac{\int_{-\frac{c\pi}{\log T}}^{\frac{c\pi}{\log T}} 2\Re\left(\sum_{mn \leq K} \frac{\lambda(m)m^{i\alpha}\Lambda(n)\lambda(mn)(mn)^{-i\alpha}}{mn} \right) d\alpha}{\sum_{n=1}^K \frac{\lambda(n)^2}{n}} \right)$$

$$= c - \frac{\left(\frac{2}{\pi} \sum_{mp \leq K} \frac{\lambda(m)\lambda(mp)\sin\left(\pi c \frac{\log n}{\log T}\right)}{mp} \right)}{\sum_{n=1}^K \frac{\lambda(n)^2}{n}} + O\left(\frac{1}{\log T}\right)$$

$$= c + \frac{\frac{2\log K}{\pi} \int_1^K \frac{\left(1-\frac{\log x}{\log K}\right)\sin\left(\pi c \frac{\log x}{\log T}\right)}{x \log x}dx}{\log K + O(1)}$$

$$= c + \frac{2}{\pi} \int_0^1 \frac{(1-u)\sin\left(\pi c u \frac{\log K}{\log T}\right)}{u}du + O\left(\frac{1}{\log T}\right)$$

$$= c + \frac{2}{\pi} \int_0^1 \frac{(1-u)\sin\left(\pi c u \theta\right)}{u}du + O\left(\frac{1}{\log T}\right).$$

With the choice $c = 0.4999$ and $\theta = 1 + 1/12$ we find that this expression equals $1.00034 + O(1/\log T)$ and thus $Q_{\varphi_1}(c,T) > 1$ as $T \to \infty$. $\qquad\square$

Discussion Here we will show the relation between $LV(\eta_0, \sigma_0, \delta_0)$ and $Ch_1(\eta_1, \sigma_1, \delta_1)$ and $Ch_2(\eta_2, \sigma_2, \delta_2)$. We will prove that $Ch_1(\eta_0, 1, \delta_1)$, plus $Ch_2(\eta_0, 1, \delta_2)$, imply $LV(\eta_0, 0, (1 + \delta)/2)$ with $\delta = \max(\delta_1, \delta_2)$.

We have that

$$\sum_{n \leq x} (\lambda_{-\alpha} * \Lambda)(n) \lambda_\alpha(n+h) = \sum_{1 \leq mp^k \leq x} \lambda(m) \lambda(mp^k + h) \left(p^k + \frac{h}{m} \right)^{i\alpha} \log p \tag{3.68}$$

$$= \sum_{k=1}^{L} \sum_{m < \sqrt{x}} \lambda(m) \sum_{p \leq (x/m)^{1/k}} \lambda(mp^k + h) \left(p^k + \frac{h}{m} \right)^{i\alpha} \log p \tag{3.69}$$

$$+ \sum_{k=1}^{L} \sum_{m \geq \sqrt{x}} \sum_{p \leq (x/m)^{1/k}} \lambda(m) \lambda(mp^k + h) \left(p^k + \frac{h}{m} \right)^{i\alpha} \log p \tag{3.70}$$

where $L = O(\log x)$. The terms $k \geq 2$ in (3.69) are estimated trivially as

$$\sum_{2 \leq k \leq L} \sum_{m \leq \sqrt{x}} \sum_{p \leq (x/m)^{1/k}} \log p \ll \sum_{2 \leq k \leq L} \sum_{m \leq \sqrt{x}} (x/m)^{1/k} \ll x^{\frac{1}{2}}.$$

For $k = 1$, we let $g(x) = (x + \frac{h}{m})^{i\alpha} \log x$ and the inner sum in (3.69) is

$$\sum_{p \leq \frac{x}{m}} \lambda(mp+h) g(p) = \left(\sum_{p \leq \frac{x}{m}} \lambda(mp+h) \right) g(\tfrac{x}{m}) - \int_1^{\frac{x}{m}} \left(\sum_{p \leq t} \lambda(mp+h) \right) g'(t) dt.$$

Using the fact that $g'(t) \ll t^{-1+\varepsilon}$ together with $Ch_2(\eta_0, 1, \delta_2)$, (3.34), we find that

$$\sum_{p \leq \frac{x}{m}} \lambda(mp+h) g(p) \ll (\tfrac{x}{m})^{\delta_2} (\tfrac{x}{m} + \tfrac{h}{m})^{i\alpha} \log(\tfrac{x}{m}) + O\left(\int_1^{x/m} t^{\delta_2 - 1 + \varepsilon} \right) \ll (\tfrac{x}{m})^{\delta_2 + \varepsilon}. \tag{3.71}$$

Thus (3.69) is bounded by

$$\ll \sum_{m \le \sqrt{x}} |\lambda(m)| (\tfrac{x}{m})^{\delta_2 + \varepsilon} + \sqrt{x} \ll x^{(1+\delta_2+\varepsilon)/2}.$$

We now estimate (3.70). We rewrite the sum as

$$\sum_{k=1}^{L} \sum_{p < x^{1/(2k)}} \log p \sum_{\sqrt{x} \le m \le x/p^k} \lambda(m) \lambda(mp^k + h) \left(p^k + \frac{h}{m} \right)^{i\alpha}.$$

Now by using $Ch_1(\eta_0, 1, \delta_1)$, (3.33), and the fact that

$$\frac{\partial}{\partial x} \left((p^k + \frac{h}{x})^{i\alpha} \right) \ll x^{-1+\varepsilon}$$

and partial summation we have that the innermost sum in (3.70) is

$$\left(\frac{x}{p^k} \right)^{\delta_1} \left(p^k + \frac{hp^k}{x} \right)^{i\alpha} \log(x) + O\left(\int_1^{x/p^k} t^{\delta_1 - 1 + \varepsilon} dt \right). \tag{3.72}$$

Therefore we have that (3.70) contributes $O(x^{(1+\delta_1+\varepsilon)/2})$ to the error term. Finally, let $\delta = \max(\delta_1, \delta_2)$, then for $h \ne 0$ we have

$$\sum_{n < x} (\lambda_{-\alpha} * \Lambda)(n) \lambda_\alpha(n + h) = O(x^{(1+\delta+\varepsilon)/2}). \tag{3.73}$$

3.4.1 Small gaps and $Q(c,T)$

In this section we give a proof of the fact that $Q(c,T) > 1$ implies $\mu \le c$. Assume that

$$Q_\varphi(c, T) = \frac{\int_{-\frac{c\pi}{\log T}}^{\frac{c\pi}{\log T}} \sum_{T/2 \le \gamma \le 2T} \varphi(\gamma + \alpha) d\alpha}{\int_{T/2}^{2T} \varphi(t) dt} > 1,$$

this means that there exist an intersection between intervals $[\gamma - \frac{c\pi}{\log T}, \gamma + \frac{c\pi}{\log T}]$ where $T/2 \le \gamma \le 2T$ are the imaginary parts of the zeros of the zeta function. Therefore we can find γ

and γ' such that

$$|\gamma - \gamma'| < \frac{2\pi c}{\log T},$$

and therefore there exist n such that

$$\gamma_n - \gamma_{n+1} = \frac{2\pi \tilde{c}}{\log T},$$

with $|\tilde{c}| < c$. Using this we have

$$
\frac{\gamma_n \log \gamma_n}{2\pi} - \frac{\gamma_{n+1} \log \gamma_{n+1}}{2\pi} = \frac{1}{2\pi} \left(\gamma_{n+1} \log \left(1 + \frac{2\pi \tilde{c}}{\gamma_{n+1} \log T} \right) \right) + \frac{\tilde{c}}{\log T} \log \left(\gamma_{n+1} + \frac{2\pi \tilde{c}}{\log T} \right)
$$

$$
= \tilde{c} + O\left(\frac{1}{\log T} \right), \tag{3.74}
$$

Since $|\gamma_{n+1} + \frac{2\pi \tilde{c}}{\log T}| < 2T + 1$. Therefore we have $|\hat{\gamma}_n - \hat{\gamma}_{n+1}| \leq |\tilde{c}| < c$. Now since we have $\mu = \liminf_{n \to \infty} \left(\hat{\gamma}_{n+1} - \hat{\gamma}_n \right)$ we conclude that $\mu < c$.

Chapter 4

On binary and quadratic divisor problems

4.1 Introduction

In this paper we are concerned with shifted convolution sums of several arithmetic functions. We divide the introduction into three parts. In the first part we discuss the binary divisor problem which plays an important role in bounding the fourth moment of the zeta function on the critical line. In the second part we discuss the quadratic divisor problem which has applications to bounding more general L-functions. In the last part of the introduction we discuss the application of the quadratic divisor problem to the Lindelöf hypothesis.

4.1.1 Binary convolution sums

The binary additive divisor problem is related to calculation of

$$\sum_{m-n=h} d(m)d(n)f(m,n), \qquad (4.1)$$

where $d(n)$ is the number of divisors of n and f is a smooth function on $\mathbb{R}^+ \times \mathbb{R}^+$ which oscillates mildly. Vinogradov [66] and Conrey and Gonek in [13] conjectured that

$$\sum_{n \leq X} d(n)d(n+h) = Main\ term + O(X^{1/2+\varepsilon}),$$

uniformly for $h \leq X^{1/2}$, where the main term is of the form $XP(\log X)$, where P is a quadratic polynomial whose coefficients are functions of h. This problem begins with Ingham, who found an asymptotic with error term $o(X)$. Estermann [24] improved the error term to $O(X^{11/12+\varepsilon})$. Using Weil's optimal bound on Kloosterman sums, Heath-Brown [35] improved the error term to $O(X^{5/6+\varepsilon})$. The final improvement on the error term with respect to X was obtained by Deshouillers and Iwaniec [17]. For fixed h they proved

$$\sum_{n \leq X} d(n)d(n+h) = \textit{Main term} + O(X^{2/3+\varepsilon}). \tag{4.2}$$

Further improvement in the h-aspect was obtained by Motohashi [62], where he proved a uniform result for $h \leq X^{64/39}$. Finally, Meurman [55] improved the range to $h \leq X^{2-\varepsilon}$. This is the best result in the literature.

In this article shifted convolution sums of the shape

$$\sum_{am-bn=h} \lambda(m)\gamma(n)f(am,bn) \tag{4.3}$$

shall be considered for sequences including the divisor function, Fourier coefficients of a primitive cusp form, and the number of representations of an integer n, as a sum of two squares. Let $g(z)$, be a primitive cusp form of weight k and level q. We have that g has a Fourier expansion

$$g(z) = \sum_{n=1}^{\infty} \alpha(n)n^{(k-1)/2}e(nz). \tag{4.4}$$

The shifted convolution sum for the Fourier coefficients $\alpha(n)$ of f is

$$\sum_{am-bn=h} \alpha(m)\alpha(n)f(am,bn). \tag{4.5}$$

Blomer [6] proved that if f is supported on $[X,2X] \times [X,2X]$ and has decaying partial derivatives satisfying

$$\frac{\partial^{i+j}}{\partial x^i \partial y^j} f(x,y) \ll \frac{1}{X^{i+j}}, \tag{4.6}$$

75

then (4.5) is $\ll X^{1/2+\theta+\varepsilon}$. Here θ is the constant such that for $\lambda(n)$ the eigenvalues of the Hecke operator that acts on the space of weight 0 Maass cusp forms of level q, we have $|\lambda(n)| \leq d(n)n^{\theta}$. The Ramanujan-Petersson conjecture predicts $\theta = 0$ and the Weil bound for Kloosterman sums gives $\theta \leq 1/4$. Kim and Shahidi [50] proved $\theta \leq 1/9$, and the current best bound is $\theta \leq 7/64$, due to Kim and Sarnak [49].

For sums of two squares we have

$$r(n) = \#\{(x,y) : x^2 + y^2 = n\} = 4\sum_{d|n}\chi_4(d),$$

where χ_4 is the non principal character modulo 4. For odd h, Iwaniec [45], by employing spectral theory, proved

$$\sum_{n \leq X} r(n)r(n+h) = 8\left(\sum_{d|h}\frac{1}{d}\right)X + O(h^{1/3}X^{2/3}),$$

and Chamizo [10] gave a conditional result for general h.

There is a major difference between sequences like $d(n)$ or $r(n)$ and $\alpha(n)$. We will explain it as follows. For $\alpha(n)$ we have

$$\sum_{n \leq X} \alpha(n)e(nx) \ll \sqrt{X}\log X,$$

while the same sum obtained by replacing $\alpha(n)$ with $d(n)$ or $r(n)$, depends on x, has main terms bigger than $\sqrt{X}$. This difference makes it harder to deal with shifted convolution sums of sequences like $d(n)$ or $r(n)$. More precisely, the circle method developed by Jutila [48] is very powerful for calculating the shifted convolution sums of coefficients of modular or Mass forms of $SL(2,\mathbb{Z})$ and even $SL(3,\mathbb{Z})$ (see [64]). However because of the difference mentioned, the Jutila circle method is not useful for shifted convolution sums of the sequences whose main terms are greater than $\sqrt{X}$. The purpose of this part of this article is to develop the δ-method of Duke and Friedlander and Iwaniec [22] in order to handle shifted

convolution sums of these sequences, with good error terms. The key ingredient is Voronoi type summation formulae which introduces Kloosterman sums via the circle method. In our work instead of using the Weil bound on Kloosterman sums we will get a better error term by means of the Kuznetsov trace formula [18, Theorem 1].

In this direction we prove

Theorem 4.1. *Let f be a smooth function supported on $[X, 2X] \times [X, 2X]$ satisfying (4.6). then for $\varepsilon > 0$ and $h \ll X^{1-\varepsilon}$, we have*

$$\sum_{m-n=h} d(m)d(n)f(m,n) = Main\ term(f) + O(X^{1/2+\varepsilon}h^{\theta}). \tag{4.7}$$

The main term is the same as [22, Equation 5] with $a, b = 1$.

Note that the Ramanujan Petersson conjecture predict that $\theta = 0$. This theorem improves on Meurman's result [55], $O(X^{1/2+\varepsilon}h^{1/8+\theta/2})$, for the weight function f satisfying (4.6). (See page 238 of [55] with $N \asymp X$.)

Another example of sequences with main terms is obtained from $\tau_{\chi}(n) = \sum_{d|n} \chi(d)$ where χ is a Dirichlet character. We prove that

Theorem 4.2. *Let χ be an odd primitive character modulo a prime number p. Let f be a smooth function supported on $[X, 2X] \times [X, 2X]$ satisfying (4.6). Then for $h \ll X^{1-\varepsilon}$, if $p|h$ we have*

$$\sum_{m-n=h} \tau_{\chi}(m)\tau_{\overline{\chi}}(n)f(m,n) = Main\ term(f) + O(X^{1/2+\theta+\varepsilon}), \tag{4.8}$$

where the Main term stated in (4.63). For the sum of two squares, if $4|h$ we have

$$\sum_{m-n=h} r(m)r(n)f(m,n) = Main\ term(f) + O(X^{1/2+\theta+\varepsilon}). \tag{4.9}$$

where the main term comes from setting $q = 4$ in (4.63).

Note that (4.8) improves, in the binary case, the error $O(X^{3/4+\varepsilon})$ obtained by Heap [34]. Our method seems to be applicable to the shifted convolution sum of the divisor function

and the Fourier coefficient of a cusp form of the full modular group and weight k. We expect the following to hold:

$$\sum_{n-m=h} \alpha(n)d(m)f(n,m) = O(X^{1/2+\varepsilon}h^{\theta}). \tag{4.10}$$

Next we look at more general shifted convolution sums.

4.1.2 Quadratic divisor problem

As we mentioned previously one application of the binary divisor problem is to bounding the moments of the zeta function. In this section we study a variation of the binary divisor problem that has applications to other families of L-functions. Let $L_g(s)$ be the L-function attached to g in (4.4), i.e.

$$L_g(s) := \sum_{n=1}^{\infty} \alpha(n)n^{-s}. \tag{4.11}$$

This L-function satisfies a functional equation from which the convexity bound

$$L_g(s) \ll (k^2|s^2|q)^{\frac{1}{4}+\varepsilon}$$

may be derived. The Lindelöf hypothesis asserts

$$L_g(s) \ll \left(k^2|s^2|q\right)^{\varepsilon}, \tag{4.12}$$

for any $\varepsilon > 0$. In many applications it suffices to replace the exponent $1/4$ by any smaller number. Such an estimate is called a subconvex bound. In order to break the convexity bound on $L_g(s)$, Duke, Friedlander and Iwaniec in [21, 20] needed an asymptotic with a good error term for $D_f(a, 1; h)$, where

$$D_f(a,b;h) := \sum_{am-bn=h} d(m)d(n)f(am,bn). \tag{4.13}$$

78

In [22] they proved that if f satisfies (4.6) then

$$D_f(a,b;h) = \text{ Main term}(f,a,b) + E_f(a,b,h), \qquad (4.14)$$

where

$$E_f(a,b,h) = O(X^{3/4+\varepsilon}).$$

Note that the main term has order of magnitude of X/ab, thus the result is nontrivial as long as $ab < X^{1/4}$. As an application of (4.14) in [21, 20] they proved that

$$L_g(\tfrac{1}{2}+it) \ll q^{47/192+\varepsilon}. \qquad (4.15)$$

In general, improving the error term or getting the error term of order $X^{1-\varepsilon}/ab$, appears to be an extremely hard problem which we discuss in the next section. The purpose of this article is to improve the error term when one of a or b equals 1. We prove the following:

Theorem 4.3. *Let Let f be a smooth function supported on $[X,2X] \times [X,2X]$ satisfying* (4.6). *For $h \ll X^{1-\varepsilon}$, We have*

$$D_f(a,1;h) := \sum_{am-n=h} d(m)d(n)f(am,n) = \text{Main term}(f,a,1) + O(X^{1/2+\theta+\varepsilon}), \quad (4.16)$$

where the Main term stated in the Equation (4.80).

Note that $\theta < 7/64 \approx 0.109375$. This unconditionally improves the error term $O(X^{0.75+\varepsilon})$ of [22] to $O(X^{0.6094})$, and under the Ramanujan-Petersson conjecture to $O(X^{0.5+\varepsilon})$.

Remark 4.4. For the application to get a subconvex bound (4.15) it is enough to take $b = 1$.

In general to detect the condition $am - bn = h$ in the sum (4.13), one needs to use some variant of the circle method. There are two major versions of the circle method that can be used in shifted convolution sums problems. The δ-method was invented by Duke,

Friedlander and Iwaniec [19] and it was used to break the convexity bound on *L*-functions associated to holomorphic cusp forms. Their idea was developed in many other papers (see [51, 56]). Another method used frequently in such problems is known as the Jutila circle method [48], which also has applications on shifted convolution sums for $GL(3) \times GL(2)$ [64]. We did not use either of these methods. In the case of the δ-method the inverses of *a* and *b* would enter in the Kloosterman sums. This would make it difficult to average the Kloosterman sums. We tried to apply Blomer's [6] treatment of the Jutila circle method to $D_f(a,b;h)$. However, despite many attempts, we were unable to make the argument work. The problem starts with [6, Lemma 3.2], which provides square root cancellation on average for shifted convolution sums of Fourier coefficient of cusp forms. We do not have such estimates for the divisor function. Here we use a more elementary method which goes back to Heath-Brown and was used by Meurman in [55]. In our argument we need to take $b = 1$, otherwise the inverse of *b* enters the Kloosterman sums and makes the averaging difficult. It might be possible to treat the case $b > 1$ by using spectral theory of automorphic forms to break the Kloosterman sums into Fourier coefficients of Maass forms. However, even if this idea works, it will greatly complicate the argument and we would like to present a simple proof.

4.1.3 Generalized shifted divisor problem

In the previous section we mentioned the connection between the quadratic divisor problem and sub-convexity bounds for families of *L*-functions. Breaking the convexity bound is a step forward towards the Lindelöf hypothesis (4.12) for these *L*-functions. Now let

$$M_k(T) = \int_0^T \left| \zeta\left(\tfrac{1}{2} + it\right) \right|^{2k} dt \qquad (4.17)$$

be the k-th moment of the Riemann zeta function. The Lindelöf hypothesis for the Riemann zeta function is equivalent to the statement that

$$M_k(T) \ll T^{1+\varepsilon}, \tag{4.18}$$

for all positive integers k and all positive real numbers ε. There is a close connection between the generalized shifted divisor problem and the moments of the zeta function. Here we define the generalized shifted divisor problem, or (k,l)-shifted divisor problem, as finding non-trivial estimates for the sum

$$\sum_{m-n=h} d_k(m)d_l(n)f(m,n), \tag{4.19}$$

where $d_k(n) = \#\{(d_1 \cdots d_k) \in \mathbb{N}^k : d_1 \cdots d_k = n\}$, and f satisfies (4.6). There are conflicting conjectures regarding the size of the error term in the (k,k)-shifted divisor problem.

Conjecture 4.5. Vinogradov [66] conjectured

$$\sum_{m-n=h} d_k(m)d_k(n)f(m,n) = Main\ term(f) + O(X^{1-\frac{1}{k}}). \tag{4.20}$$

Furthermore, Ivic [44] suggested that the O term in (4.20) should be replaced by Ω. Contrary to Ivic's conjecture, Conrey and Gonek's [13] conjectured the following.

$$\sum_{m-n=h} d_k(m)d_k(n)f(m,n) = Main\ term(f) + O(X^{\frac{1}{2}+\varepsilon}), \tag{4.21}$$

uniformly for $h \leq \sqrt{X}$. Note that in their formulation of the conjecture, f is the indicator function of $[X,2X] \times [X,2X]$. However in practice we need to consider f as in (4.6). Ivic's conjecture in the case $k=2$ was proven by Motohashi [62] and Szydlo improved the result and showed the error term in the case $k=2$ is $\Omega_{\pm}(X^{1/2})$.

We mentioned some of the results for the $(2,2)$-shifted divisor problem in the first part

of the introduction. For $k, l > 2$ this problem remains unsolved and seems to be extremely hard. For the case $(k, l) = (3, 2)$ an asymptotic formula was obtained by Hooley [39]. For the case $(k, 2)$ an asymptotic formula was derived by Linnik [54] using the dispersion method. Motohashi improved on Linnik's result by saving a power of $\log X$ in the error term. A power savings in the error term was obtained by Friedlander and Iwaniec [26] in the case $(k, l) = (3, 2)$. They showed that there exists $\delta > 0$ such that the error term is smaller than $X^{1-\delta}$. Heath-Brown [36] showed that $\delta = 1/102$ is valid.

Here we describe a bridge between the quadratic divisor problem and the (k, l)-shifted divisor problem. We explain this by means of the following lemma.

Lemma 4.6. *Let f be a compactly supported function defined on $\mathbb{R}^2$. We have that*

$$\sum_{a,b} D_f(a,b;h) = \sum_{a,b} \sum_{am-bn=h} d(m)d(n)f(am,bn) = \sum_{m-n=h} d_3(m)\, d_3(n)\, f(m,n). \quad (4.22)$$

In general for $k, l \geq 2$ we have

$$\sum_{\substack{a_i \\ 1 \leq i \leq k-1}} \sum_{\substack{b_j \\ 1 \leq j \leq l-1}} \sum_{a_1 \cdots a_{k-1} n - b_1 \cdots b_{l-1} m = h} d(n)\, d(m)\, f(a_1 \cdots a_{k-1} n,\ b_1 \cdots b_{l-1} m)$$

$$= \sum_{m-n=h} d_k(m)\, d_l(n)\, f(m,n). \quad (4.23)$$

This lemma shows that by summing $D_f(a,b;h)$ over a and b we can study the generalized shifted divisor problem. Therefore the error term in the (k, l)-shifted divisor problem is the sum of the error terms in the quadratic divisor problem. This brings us to the following crucial question.

Question: What is the size of the error $E_f(a,b,h)$?

We may assume the following plausible assumptions:

1. The function E as a function of a, b oscillates mildly with respect to changes in a, b. This means that if $\| (a,b) - (c,d) \|_2$ is small then $E_f(a,b,h)$ and $E_f(c,d,h)$ are roughly the same size.

2. For $a, b \ll 1$, $E_f(a, b, h) = O(X^{1/2+\varepsilon})$.

3. We assume that it possible to restrict the sum of $E_f(a, b, h)$ over a, b in (4.22) to the region $ab \ll X$.

Using these heuristics we may conclude that either $E_f(a, b, h) = O(\sqrt{X}/ab)$ or $E_f(a, b, h) = O(\sqrt{X/ab})$. Note that $E_f(a, b, h) = O(\sqrt{X}/ab)$ matches very well with Conrey and Gonek's conjecture for (k, k)-shifted divisor problem (4.21). While assuming $E_f(a, b, h) = O(\sqrt{X/ab})$ only matches Vinogradov's conjecture for $(3, 3)$-shifted divisor problem. Moreover, to get Vinogradov's conjecture (4.20) for general k one needs to assume specific cancellations between $E_f(a, b, h)$ when we sum over a, b. This argument shows that the conjecture of Conrey and Gonek on the order of magnitude of the error terms in (k, k)-shifted divisor problem seems to be more accurate than Vinogradov's and Ivic's conjectures.

We conclude this section with pointing out the connection between the (k, k)-shifted divisor problem and the Lindelöf hypothesis for the Riemann zeta function. Ivic [44] has shown that if (4.20) holds for $k = 3$ then (4.18) holds for $k = 3$. Moreover, in [43] he proved that if we assume that the error term, on average over h in (4.21), has square root cancellation, then the Lindelöf hypothesis for the Riemann zeta function would follow.

Structure of the paper and notation. We will proceed first with introducing the δ-method and then using the Voronoi summation formulas to form Kloosterman sums. After that we will prove the necessary conditions that are needed for using the Kuznetsov formula in averaging the Kloosterman sums. We conclude the paper by treating the quadratic divisor problem with a different formulation but somehow similar with the method used in the binary divisor problem. Note that throughout the paper we consider $h \ll X^{1-\varepsilon}$.

Kloosterman sums. Let m, n, q be natural numbers and $e(x) = e^{2\pi i x}$. The sum

$$S(m,n;q) = \sum_{\substack{1 \leq x < q \\ (x,q)=1}} e\left(\frac{mx + n\bar{x}}{q}\right) \tag{4.24}$$

where $x\bar{x} \equiv 1 \pmod{q}$, is called the Kloosterman sum. Weil [68] proved that

$$S(m,n;q) \leq d(q)\sqrt{\gcd(m,n,q)}\sqrt{q}.$$

Although the Weil bound is optimal, on average the Kloosterman sum has a size about q^ε. This follows from Kuznetsov's formula which is a certain average of $S(m,n;q)$ over q. Our use of kuznetsov's formula instead of the Weil bound the key tools used in this article.

Bessel functions. Throughout this article we make extensive use of the standard Bessel functions. They are defined as follows:

$$J_n(z) = \sum_{k=0}^{\infty} \frac{(-1)^k (z/2)^{2k+n}}{k!(n+k)!},$$

$$Y_n(z) = -\sum_{k=0}^{n-1} \frac{(n-k-1)!}{\pi k!}(z/n)^{2k-n} + \sum_{k=0}^{\infty} \frac{(-1)^k(n-k-1)!}{\pi k!}\left(2\log(z/2) - \frac{\Gamma'}{\Gamma}(k+1) - \frac{\Gamma'}{\Gamma}(k+n+1)\right),$$

$$K_n(z) = \frac{1}{2}\sum_{k=0}^{n-1} \frac{(-1)^k(n-k-1)!}{k!}(z/n)^{2k-n}$$

$$+ \frac{(-1)^{n-1}}{2}\sum_{k=0}^{\infty} \frac{(-1)^k(n-k-1)!}{k!}\left(2\log(z/2) - \frac{\Gamma'}{\Gamma}(k+1) - \frac{\Gamma'}{\Gamma}(k+n+1)\right).$$

Moreover we use the following properties. $\left(z^\nu Y_\nu(z)\right)' = z^\nu Y_{\nu-1}(z)$, $\left(z^\nu K_\nu(z)\right)' = -z^\nu K_{\nu-1}(z)$, and $\left(z^\nu J_\nu(z)\right)' = z^\nu J_{\nu-1}(z)$. We also use the following bounds from [51, Lemma C.2]. For $z > 0$ and $k \geq 0$

$$\left(\frac{z}{1+z}\right)^i Y_0^{(i)}(z) \ll \frac{(1 + |\log z|)}{(1+z)^{1/2}}, \tag{4.25}$$

$$\left(\frac{z}{1+z}\right)^i K_0^{(i)}(z) \ll \frac{e^{-z}(1 + |\log z|)}{(1+z)^{1/2}}. \tag{4.26}$$

For further properties of Bessel functions see [52].

4.2   δ-method

In this section we follow [22] to introduce and set up the δ-method. Let $Q > 0$ and $w(u)$ be an even, smooth, compactly supported function on $Q \leq |u| \leq 2Q$ and

$$w^{(i)}(u) \ll \frac{1}{Q^{i+1}}, \quad \sum_{q=1}^{\infty} w(q) = 1. \tag{4.27}$$

The δ function is defined on $\mathbb{Z}$ by $\delta(0) = 1$ and $\delta(m) = 0$ for $m \neq 0$. The δ-method gives a decomposition of the δ function in terms of additive characters $e(\cdot)$ on rational numbers. More precisely we have:

$$\delta(m) = \sum_{q=1}^{\infty} \sum_{(d,q)=1} e\Big(\frac{md}{q}\Big) \Delta_q(m), \tag{4.28}$$

where

$$\Delta_q(m) = \sum_{r=1}^{\infty} \frac{w(qr) - w(\frac{m}{qr})}{qr}.$$

Let $f(x,y)$ be a differentiable function supported in $[X, 2X] \times [X, 2X]$ satisfying (4.6). Let ϕ be a smooth function supported on $[-X, X]$ with the property that $\phi^{(i)} \ll X^{-i}$. By applying (4.28) to detect the condition $m - n = h$ in (4.7) we have

$$\sum_{m-n=h} d(m)d(n)f(m,n) = \sum_{q<Q} \sum_{d \bmod q}^{*} e\Big(\frac{-hd}{q}\Big) \sum_{m,n} d(m)d(n)e\Big(\frac{dm-dn}{q}\Big)E(m,n,q), \tag{4.29}$$

where

$$E(x,y,q) = f(x,y)\phi(x-y-h)\Delta_q(x-y-h). \tag{4.30}$$

For the left hand side of (4.8), (4.9) and (4.10) we have similar formula.

4.3 Voronoi summation formulas

Let $f(n)$ be an arithmetic function, let q be an integer, and let $g(n)$ be a compactly supported function on $\mathbb{R}^+$. For $(d,q) = 1$ we have

$$\sum_n f(n)e\left(\frac{nd}{q}\right)g(n) = \sum_{a \bmod q} e\left(\frac{a}{q}\right) \sum_{n \equiv \bar{d}a \bmod q} f(n)g(n) \qquad (4.31)$$

where $\bar{d}d \equiv 1 \pmod{q}$. Now if for $a \neq 0$, $f(n)$ has some sort of well distribution modulo q one can study the main term and the error term in (4.31). The general Voronoi summation formula studies the sum of the type (4.31) for certain sequences. The idea started with Voronoi in [67]. Here we state the Voronoi summation formula for $d(n), \tau_\chi(n), r(n)$ and $\alpha(n)$.

Lemma 4.7. *Let $g(x)$ be a smooth, compactly supported function on $\mathbb{R}^+$ and let $(d,q) = 1$. We have*

$$\sum_{n=1}^{\infty} d(n)e\left(\frac{nd}{q}\right)g(n) = \frac{1}{q}\int_0^{\infty}(\log x + 2\gamma - \log q)g(x)dx + \sum_{i=1}^{2}\sum_{n=1}^{\infty} e\left(\frac{\pm n\bar{d}}{q}\right)g_i(n), \qquad (4.32)$$

where

$$g_1(n) = -\frac{2\pi}{q}\int_0^{\infty} g(x)Y_0\left(\frac{4\pi\sqrt{nx}}{q}\right)dx$$

$$g_2(n) = \frac{4}{q}\int_0^{\infty} g(x)K_0\left(\frac{4\pi\sqrt{nx}}{q}\right)dx.$$

If $(c,q) = 1$, for $\tau_\chi(n)$, where χ is an odd Dirichlet character modulo c, we have

$$\sum_{n=1}^{\infty} \tau_\chi(n)e\left(\frac{nd}{q}\right)g(n) = \frac{\chi(q)}{q}L(1,\chi)\int_0^{\infty} g(x)dx \qquad (4.33)$$

$$- 2\pi\frac{\chi(q)}{q}\frac{\tau(\chi)}{c}\sum_{n=1}^{\infty} \tau_\chi(n)e\left(\frac{-n\bar{d}c}{q}\right)\int_0^{\infty} g(x)J_0\left(\frac{4\pi\sqrt{nx}}{\sqrt{cq}}\right)dx,$$

if $c|q$ we have

$$\sum_{n=1}^{\infty} \tau_{\chi}(n)e\left(\frac{nd}{q}\right)g(n) = \frac{\chi(\bar{d})}{q}\tau(\chi)L(1,\bar{\chi})\int_0^{\infty}g(x)dx \tag{4.34}$$
$$- 2\pi i\frac{\chi(\bar{d})}{q}\sum_{n=1}^{\infty}\tau_{\chi}(n)e\left(\frac{-n\bar{d}}{q}\right)\int_0^{\infty}g(x)J_0\left(\frac{4\pi\sqrt{nx}}{q}\right)dx,$$

and if $c = 4$ and $q \equiv 2 \pmod 4$ we have

$$\sum_{n=1}^{\infty} r(n)e\left(\frac{nd}{q}\right)g(n) = -2\pi i\frac{\chi(\bar{d})}{q}\sum_{n=1}^{\infty}r^*(n)e\left(\frac{-n\bar{d}}{2q}\right)\int_0^{\infty}g(x)J_0\left(\frac{4\pi\sqrt{nx}}{q\sqrt{2}}\right)dx, \tag{4.35}$$

where

$$r^*(n) = \sum_{m_1 m_2 = n} \chi_4(m_1)\left(1 - (-1)^{m_1}\right) \tag{4.36}$$

Finally, for Fourier coefficients of weight k cusp form we have

$$\sum_{n=1}^{\infty} \alpha(n)e\left(\frac{nd}{q}\right)g(n) = \frac{-2\pi i^k}{q}\sum_{n=1}^{\infty}\alpha(n)e\left(\frac{-n\bar{d}}{q}\right)\int_0^{\infty}g(x)J_{k-1}\left(\frac{4\pi\sqrt{nx}}{q}\right)dx. \tag{4.37}$$

Here Y_0, K_0 and J_k are Bessel functions.

The formula for $d(n)$ is due to Jutila [47]. The formula for $\alpha(n)$ and $\tau_{\chi}(n)$ in the case $(c,q) = 1$ and $c|q$ can be found in Chapter 4 of [46]. Here we would give a proof for the case $c = 4$ and $q \equiv 2 \pmod 4$.

Proof of Lemma 4.7. Let χ_4 be the non principal odd character modulo 4. We have

$$\sum_{n} r(n)e\left(\frac{nd}{q}\right)g(n) = \sum_{n}\sum_{m_1 m_2 = n}\chi_4(m_1)e\left(\frac{m_1 m_2 d}{q}\right)g(m_1 m_2). \tag{4.38}$$

We set $m_1 = 2n_1 q + u_1$ and $m_2 = n_2 q + u_2$. Since $q \equiv 2 \pmod 4$, with this choice of m_1 we have $\chi_4(m_1) = \chi_4(u_1)$ and therefore (4.38) is equal to

$$\sum_{\substack{u_1 \bmod 2q \\ u_2 \bmod q}}\sum_{n_1, n_2}\chi_4(u_1)e\left(\frac{u_1 u_2 d}{q}\right)g\left((u_1 + 2qn_1)(u_2 + qn_2)\right) \tag{4.39}$$

We apply the Poisson summation formula (Equation (4.24) of [46]) to the sum over n_1, n_2. Therefore, (4.39) is equal to

$$\frac{1}{2q^2} \sum_{m_1, m_2} \sum_{\substack{u_1 \bmod 2q \\ u_2 \bmod q}} \chi_4(u_1) e\left(\frac{u_1 u_2 d}{q} + \frac{m_2 u_2}{q} + \frac{m_1 u_1}{2q}\right) \hat{g}\left(\frac{m_1}{\sqrt{2}q}, \frac{m_2}{\sqrt{2}q}\right), \qquad (4.40)$$

where

$$\hat{g}\left(\frac{m_1}{\sqrt{2}q}, \frac{m_2}{\sqrt{2}q}\right) = \int_0^\infty \int_0^\infty g(xy) e\left(\frac{-m_1 x}{\sqrt{2}q}\right) e\left(\frac{-m_2 y}{\sqrt{2}q}\right) dx dy.$$

Note that $\sqrt{2}$ in the denominator comes from the change of variable inside the above integral. Now the sum over u_2 inside (4.40) is zero unless $u_1 \equiv \bar{d} m_2 \pmod{q}$, in which case the sum is equal to q. Since we considered u_1 modulo $2q$ we have only choices $\bar{d} m_2, \bar{d} m_2 + q$ for u_1. Considering this (4.40) is equal to

$$\frac{1}{2q} \sum_{m_1, m_2} \left(\chi_4(\bar{d} m_2) e\left(\frac{m_1 m_2 \bar{d}}{2q}\right) + (-1)^{m_1} \chi_4(\bar{d} m_2 + q) e\left(\frac{m_1 m_2 \bar{d}}{2q}\right)\right) \hat{g}\left(\frac{m_1}{\sqrt{2}q}, \frac{m_2}{\sqrt{2}q}\right) \quad (4.41)$$

The rest of the proof follows exactly the proof of Theorem 4.14 in [46]. Note that in the case $q \equiv 2 \pmod 4$ we do not have a main term because the main term comes from setting m_1 or m_2 equal to zero. For $m_1 = 0$ we get $\chi_4(\bar{d} m_2) + \chi_4(\bar{d} m_2 + q)$ inside the parenthesis in (4.41), which is equal to zero since $q \equiv 2 \pmod 4$. For $m_2 = 0$ we have both $\chi_4(\bar{d} m_2)$ and $\chi_4(\bar{d} m_2 + q)$ are equal to zero. $\qquad \square$

Next we apply the Voronoi summation formula (4.32) to the rigt hand side of (4.29). Similarly we use Lemma (4.7) equations (4.33), (4.34) and (4.35) for (4.8), (4.9).

4.4 Toward Kloosterman sums

In this part we apply the Voronoi summation formula (Lemma 4.7) to the sums we derived from the δ-method. This will lead to the Kloosterman sums inside our formula for the error terms. Our final aim is to average the Kloosterman sums and obtain sharp estimates for the error terms. For $\tau_\chi(n)$ we will work out the formula in detail. For the

shifted convolution of $r(n)$ in (4.9), and the shifted convolution of $d(n)$ and $\alpha(n)$ in (4.10), we will give the final formula. As for the divisor function, we will write the result for $d(n)$ using [22, Equation (24)]. We consider the general case a, b not necessarily equal to 1 to explain why our argument cannot be applied to the quadratic divisor problem.

4.4.1 Formula for τ_χ

By using the δ-method we have

$$\sum_{m-n=h} \tau_\chi(m)\overline{\tau_\chi(n)}f(m,n) = \tag{4.42}$$

$$\sum_{q<Q}\sideset{}{^*}\sum_{d \bmod q} e\left(\frac{-hd}{q}\right) \sum_{m,n} \tau_\chi(m)\overline{\tau_\chi(n)}e\left(\frac{dm-dn}{q}\right)E(m,n,q).$$

Recall that $E(\cdot,\cdot,\cdot)$ is defined in (4.30). First we split the sum over q into two cases: $(p,q) = 1$ and $p|q$. For $(p,q) = 1$ we apply (4.33) first to the sum over n and we end up with two terms. Then we apply (4.33) to the sum over m and we get two other terms. Consequently we have

$$\sum_{\substack{q<Q \\ (p,q)=1}}\sideset{}{^*}\sum_{d \bmod q} e\left(\frac{-hd}{q}\right) \sum_{m,n} \tau_\chi(m)\overline{\tau_\chi(n)}e\left(\frac{dm-dn}{q}\right)E(m,n,q)$$

$$= \sum_{\substack{q<Q \\ (p,q)=1}}\sideset{}{^*}\sum_{d \bmod q} e\left(\frac{-hd}{q}\right)\frac{|\chi(q)|^2}{q^2}L(1,\chi)^2 \int_0^\infty \int_0^\infty E(x,y,q)dxdy \tag{4.43}$$

$$+ \sum_{\substack{q<Q \\ (p,q)=1}}\sideset{}{^*}\sum_{d \bmod q} e\left(\frac{-hd}{q}\right)\left(2\pi\frac{|\chi(q)|^2}{q^2}\frac{\tau(\chi)}{p}L(1,\chi)\sum_{m=1}^\infty \tau_\chi(n)e\left(\frac{-m\overline{dp}}{q}\right)\int_0^\infty \int_0^\infty E(x,y,q)J_0\left(\frac{4\pi\sqrt{mx}}{q\sqrt{p}}\right)dxdy\right.$$

$$-2\pi\frac{|\chi(q)|^2}{q^2}\frac{\tau(\chi)}{p}L(1,\chi)\sum_{n=1}^\infty \overline{\tau_\chi(n)}e\left(\frac{-n\overline{dp}}{q}\right)\int_0^\infty \int_0^\infty E(x,y,q)J_0\left(\frac{4\pi\sqrt{ny}}{q\sqrt{p}}\right)dxdy + (2\pi)^2\frac{|\chi(q)|^2}{q^2}\left(\frac{\tau(\chi)}{p}\right)^2$$

$$\times \sum_{m,n=1}^\infty \tau_\chi(m)\overline{\tau_\chi(n)}e\left(\frac{-(m+n)\overline{dp}}{q}\right)\int_0^\infty \int_0^\infty E(x,y,q)J_0\left(\frac{4\pi\sqrt{mx}}{q\sqrt{p}}\right)J_0\left(\frac{4\pi\sqrt{ny}}{q\sqrt{p}}\right)dxdy\left.\right).$$

Now since we assumed that $p|h$ we write $h = h'p$. For $p|q$ we apply (4.34) in Lemma 4.7 once to the sum over m and once to the sum over n. Therefore, when $p|q$ (4.42) is equal to

$$
\sum_{\substack{q<Q \\ p|q}} \sideset{}{^*}\sum_{d \bmod q} e\left(\frac{-hd}{q}\right) \frac{|\chi(\overline{d})|^2}{q^2} \tau^2(\chi) L(1,\overline{\chi})^2 \int_0^\infty \int_0^\infty E(x,y,q) dx dy \tag{4.44}
$$

$$
+ \sum_{\substack{q<Q \\ p|q}} \sideset{}{^*}\sum_{d \bmod q} e\left(\frac{-hd}{q}\right) \left(2\pi i \frac{|\chi(\overline{d})|^2}{q^2} \tau(\chi) L(1,\overline{\chi}) \sum_{m=1}^\infty \tau_\chi(m) e\left(\frac{-m\overline{d}}{q}\right) \int_0^\infty \int_0^\infty E(x,y,q) J_0\left(\frac{4\pi\sqrt{mx}}{q}\right) dx dy \right.
$$

$$
+ 2\pi i \frac{|\chi(\overline{d})|^2}{q^2} \tau(\chi) L(1,\overline{\chi}) \sum_{n=1}^\infty \overline{\tau_\chi(n)} e\left(\frac{-n\overline{d}}{q}\right) \int_0^\infty \int_0^\infty E(x,y,q) J_0\left(\frac{4\pi\sqrt{ny}}{q}\right) dx dy
$$

$$
+ (2\pi i)^2 \frac{|\chi(\overline{d})|^2}{q^2} \sum_{m,n=1}^\infty \tau_\chi(m) \overline{\tau_\chi(n)} e\left(\frac{-(m+n)\overline{d}}{q}\right) \int_0^\infty \int_0^\infty E(x,y,q) J_0\left(\frac{4\pi\sqrt{mx}}{q}\right) J_0\left(\frac{4\pi\sqrt{ny}}{q}\right) dx dy \left. \right).
$$

4.4.2 Formula for the sum of two squares

For $r(n)$ we have a formula similar to (4.42) with $\tau_\chi(\cdot)$ replaced by $r(\cdot)$. Here we have to split the summation over q to three cases: $4|q$, $(4,q) = 1$ and $q \equiv 2 \pmod 4$. For the first two cases the final formula would be the same as (4.43) and (4.44) with $p = 4$ and $\tau_\chi(\cdot) = r(\cdot)$. The case we need to work out is $q \equiv 2 \pmod 4$. Let r^* be as (4.36). Then the corresponding formula to (4.42) for $r(n)$ is

$$
\sum_{\substack{q<Q \\ q\equiv 2 \ (\bmod 4)}} \sideset{}{^*}\sum_{d \bmod q} e\left(\frac{-hd}{q}\right) \left(\frac{|\chi(\overline{d})|^2}{q^2} (2\pi i)^2 \right. \tag{4.45}
$$

$$
\sum_{m,n=1}^\infty r^*(m) r^*(n) e\left(\frac{-(m+n)\overline{d}}{2q}\right) \int_0^\infty \int_0^\infty E(x,y,q) J_0\left(\frac{4\pi\sqrt{mx}}{\sqrt{2}q}\right) J_0\left(\frac{4\pi\sqrt{ny}}{\sqrt{2}q}\right) dx dy \left. \right).
$$

Note that since $r^*(n) = 0$ for even n, we can write the sum over m,n in (4.44) in terms of odd m,n. Therefore $(m+n)/2$ is an integer and with this we will have our Kloosterman sums.

4.4.3 Formula for the divisor function

For the shifted convolution sum of $d(n)$, i.e. equation (4.13), using [22, Equation (24)] we have

$$D_f(a,b;h) = \text{Main term}(f) + \mathcal{E}_1(a,b) + \mathcal{E}_2(a,b) + \sum_{j=3}^{8} \mathcal{E}_j(a,b), \qquad (4.46)$$

where

$$\text{Main term}(f) = \sum_{q<Q} \frac{(ab,q)}{q^2} S(h,0;q) \int_0^\infty \int 0^\infty f(\log(ax) - \lambda_{a,q})(\log(by) - \lambda_{b,q}) E(x,y,q)dxdy,$$

$$\mathcal{E}_1(a,b) = \sum_{q<Q} \frac{(ab,q)}{q^2} \left(\sum_{m=1}^{\infty} d(m)S(h,-(b,q)\overline{b_q}m;q)I_b(m,q) + \sum_{n=1}^{\infty} d(n)S(h,(a,q)\overline{a_q}n;q)I_a(n,q) \right),$$

$$\mathcal{E}_2(a,b) = \sum_{q<Q} \frac{(ab,q)}{q^2} \sum_{m,n=1}^{\infty} d(m)d(n)S(h,(a,q)\overline{a_q}m - (b,q)\overline{b_q}n;q)I_{ab}(m,n,q). \qquad (4.47)$$

Also $a_q = a/(a,q)$ and $\overline{a_q}$ is the inverse of a_q modulo q and

$$I_{ab}(m,n,q) = 4\pi^2 \int_0^\infty \int_0^\infty Y_0\left(\frac{4\pi(a,q)\sqrt{mx}}{q}\right)Y_0\left(\frac{4\pi(b,q)\sqrt{ny}}{q}\right)E(x,y,q)dxdy, \qquad (4.48)$$

and

$$I_a(m,q) = -2\pi \int_0^\infty \int_0^\infty Y_0\left(\frac{4\pi(a,q)\sqrt{mx}}{q}\right)(\log(by) - \lambda_{b,q})E(x,y,q)dxdy \qquad (4.49)$$

$$I_b(n,q) = -2\pi \int_0^\infty \int_0^\infty (\log(ax) - \lambda_{a,q})Y_0\left(\frac{4\pi(b,q)\sqrt{ny}}{q}\right)E(x,y,q)dxdy, \qquad (4.50)$$

and $\lambda_{a,q} = 2\gamma + \log\frac{aq^2}{(a,q)^2}$. The term $\sum_{j=3}^{8} \mathcal{E}_j(a,b)$ corresponds to five more error terms involving a K_0-Bessel function that are similar to $\mathcal{E}_1, \mathcal{E}_2$. Our aim is to show that

$$\mathcal{E}_1(1,1), \mathcal{E}_2(1,1) \ll X^{1/2+\varepsilon}h^\theta.$$

Remark 4.8. In [22, Equation (24)] there is a typo. Instead of $(a,q)\overline{a_q}$ they have $\overline{a}$, inside the Kloosterman sums. We would also like to emphasize that we cannot prove our result for

$D_f(a,b;h)$ for $a,b \neq 1$ because the term $\overline{a_q}$ enters into the Kloosterman sums. Ultimately, this will make the averaging impossible. The advantage of Jutila circle method [48] is that the sum over q can be restricted to the multiples of ab, while in the δ-method the sum over q runs over all integers less than Q. However, it seems difficult to apply Jutila's circle method to the divisor function as it does not have square root cancellation while the sum of the coefficients coming from holomorphic or cusp forms has square root cancellation, see [6].

Here we just deal with the error term $\mathcal{E}_2(a,b)$. The error term $\mathcal{E}_1(a,b)$ can be handled similarly. As for error terms $\mathcal{E}_j(a,b)$, $3 \leq j \leq 8$, that arise from the K_0-Bessel function, can be handled by the similarity between the K_0 and Y_0-Bessel functions. We set $a,b = 1$ and write $I(m,n,q)$ in a place of $I_{ab}(m,n,q)$.

4.5 Bounding $I(m,n,q)$

In this section we make the necessary adjustments in order to be able to use results regarding averaging Kloosterman sums. The main difficulty in proving the fact that $I(m,n,q)$ oscillates mildly with respect to q, comes from small q. In [22] the parameter Q, in the δ-method, is equal to $2\sqrt{X}$. If we use the same choice of Q and follow the method in [22, Equation (30)] for $q \ll 1$ we get the bound $I(m,n,q) \ll \sqrt{X}$, while we need $I(m,n,q) \ll X^\varepsilon$. We overcome this difficulty by changing the parameter Q from $\sqrt{X}$ to

$$Q = X^{1/2+\varepsilon}.$$

As a result we have to consider a wider range for the sum over q in (4.47). However, the faster rate of decay of the partial derivatives of w in the δ-method will help us to show that $I(m,n,q)$ is very small for $q < X^{\frac{1}{2}-\varepsilon}$. Let $I(m,n,q)$ be as (4.48) with $a = b = 1$,

$$I(m,n,q) = 4\pi^2 \int_0^\infty \int_0^\infty Y_0\left(\frac{4\pi\sqrt{mx}}{q}\right) Y_0\left(\frac{4\pi\sqrt{ny}}{q}\right) E(x,y,q)dxdy.$$

We will prove the following lemmas to show that the contribution of small q's in (4.47) are negligible. We will also find upper bounds for the range of the sum over n in (4.47). We will consider $I(m,n,q)$ with a Y_0−Bessel function, but the same lemmas are valid with replacing Y_0 with J_0−Bessel function.

Lemma 4.9. *For $\varepsilon > 0$ there exist $i, j \in \mathbb{N}$ such that, for $q < X^{1/2-\varepsilon}$ we have*

$$I(m,n,q) \ll m^{-i/2-1/4}n^{-j/2-1/4}X^{-1}$$

and

$$I(n,q) \ll n^{-j/2}X^{-1}.$$

Proof. We begin with a change of variable in $I(m,n,q)$. Setting $u = \dfrac{4\pi\sqrt{mx}}{q}$ and $v = \dfrac{4\pi\sqrt{ny}}{q}$ in the expression for $I(m,n,q)$ yields

$$I(m,n,q) = \frac{4\pi^2 q^4}{(4\pi)^4 mn} \int_0^\infty \int_0^\infty uY_0(u)vY_0(v)E\left(\frac{u^2q^2}{(4\pi)^2m}, \frac{v^2q^2}{(4\pi)^2n}, q\right)dudv. \qquad (4.51)$$

By employing the recursive formula $(z^v Y_v(z))' = z^v Y_{v-1}(z)$ and integration by parts in (4.51) we have

$$I(m,n,q) \asymp \frac{q^{2(i+j+2)}}{m^{i+1}n^{j+1}} \int_0^\infty \int_0^\infty u^{i+1}Y_i(u)v^{j+1}Y_j(v)E^{(i,j,0)}\left(\frac{u^2q^2}{(4\pi)^2m}, \frac{v^2q^2}{(4\pi)^2n}, q\right)dudv. \qquad (4.52)$$

Similarly, by integrating by parts in (4.49), for $I(n,q)$ we deduce that

$$I(n,q) \asymp \frac{q^{2(j+1)}}{n^{j+1}} \times \int_0^\infty \int_0^\infty (\log x - \lambda_q)v^{j+1}Y_j(v)E^{(0,j,0)}\left(x, \frac{v^2q^2}{(4\pi)^2n}, q\right)dxdv.$$

Here we need to estimate the partial derivatives of $E(x,y,q)$. Recall that $E(x,y,q) = f(x,y)\phi(x-$

$y-h)\Delta_q(x-y-h)$, and for the partial derivatives of E we have

$$E^{(i,j,0)} := \frac{\partial^{i+j}}{\partial x^i \partial y^j} E(x,y,q) = \sum_{\substack{r,r',s,s' \geq 0 \\ r+r'=i \\ s+s'=j}} c_{r,r',s,s'} (f\phi)^{(r,s)} \Delta_q^{(r',s')}. \tag{4.53}$$

For the partial derivative of f and Δ_q, we have $(f\phi)^{(r,s)} \ll X^{-r-s}$ and $\Delta_q^{(r',s')} \ll (qQ)^{-r'-s'-1}$. Now since $q < X^{1/2-\varepsilon}$ we have $qQ < X$, so the major term in (4.53) is $\Delta_q^{(i,j)}$. Therefore we have $E^{(i,j,0)} \ll (qQ)^{-i-j-1}$. We will apply this bound for $E^{(i,j,0)}$ together with $Y_i(u) \ll \frac{1}{\sqrt{u}}$ in (4.52) to get

$$I(m,n,q) \ll \frac{q^{2(i+j+2)}}{m^{i+1}n^{j+1}(qQ)^{i+j+1}} \int_{\frac{\sqrt{mX}}{q}}^{\frac{\sqrt{2mX}}{q}} \int_{\frac{\sqrt{nX}}{q}}^{\frac{\sqrt{2nX}}{q}} u^{i+\frac{1}{2}} v^{j+\frac{1}{2}} \, du \, dv \tag{4.54}$$

$$\ll_{i,j} \frac{q^{2(i+j+2)} X^{(i+j+3)/2} m^{i/2+3/4} n^{j/2+3/4}}{m^{i+1}n^{j+1}(qQ)^{i+j+1} q^{i+j+3}} \ll_{i,j} \frac{X^{(i+j+3)/2}}{m^{i/2+1/4} n^{j/2+1/4} Q^{i+j+1}}.$$

A similar argument for $I(n,q)$ yields:

$$I(n,q) \ll \frac{X^{(j+4)/2}}{n^{j/2} Q^{j+1}}.$$

Now, using $Q = X^{1/2+\varepsilon}$ and $j = \lfloor \frac{3}{\varepsilon} \rfloor$ completes the proof. $\qquad\square$

The following lemma will provide the bound for the sum over m,n in Equation (24) in [22]

Lemma 4.10. *For $X^{1/2-\varepsilon} < q < X^{1/2+\varepsilon}$, the contribution of $m,n > X^{3\varepsilon}$ in (4.47) is $O(X^{-1/2})$.*

Proof. Since $X^{1/2-\varepsilon} < q < X^{1/2+\varepsilon}$, we have $\frac{1}{qQ} > \frac{1}{X}$. Therefore $E^{(i,j,0)} \ll X^{-i-j-1}$. We are using same bounds as Lemma 4.9 in (4.52) and consequently

$$I(m,n,q) \ll_{i,j} \frac{q^{2(i+j+2)} X^{(i+j+3)/2} m^{i/2+3/4} n^{j/2+3/4}}{m^{i+1}n^{j+1} X^{i+j+1} q^{i+j+3}}$$

$$\ll_{i,j} \frac{q^{i+j+1} X^{(i+j+3)/2}}{m^{i/2+1/4} n^{j/2+1/4} X^{i+j+1}}.$$

Now using $q < X^{1/2+\varepsilon}$ we get $I(m,n,q) \ll_{i,j} X^{\varepsilon(i+j+1)+1} m^{-i/2-1/4} n^{-j/2-1/4}$. Similarly for

$I(n,q)$ we have that $I(n,q) \ll_j X^{\varepsilon(j+1)+1} n^{-j/2}$. And therefore by taking $j = \lfloor \frac{3}{\varepsilon} \rfloor$ we have

$$\sum_{m,n > X^{3\varepsilon}} d(m)d(n)I(m,n,q) \ll_{i,j} \frac{X}{X^{\varepsilon(i+j-3)/2}} \ll \frac{1}{\sqrt{X}}.$$

The same bound for the sum over $I(n,q)$ holds. Using this in (4.47) combined with the trivial bound on the Kloosterman sums gives us the error term of order $O(X^{-1/2+\varepsilon})$. This shows the the contribution of $m,n > X^{3\varepsilon}$ is negligible and we only need to consider the sum over m,n in (4.47) up to $X^{3\varepsilon}$. This finishes the proof of the Lemma. $\qquad\square$

It follows from Lemma 4.9 and 4.10 that

$$\mathcal{E}_2(1,1) = \sum_{X^{1/2-\varepsilon} < q < X^{1/2+\varepsilon}} \frac{1}{q^2} \sum_{m,n < X^{3\varepsilon}} d(m)d(n)S(h,m-n;q)I(m,n,q) + O(\frac{1}{\sqrt{X}}),$$

and a similarly

$$\mathcal{E}_1(1,1) = \sum_{X^{1/2-\varepsilon} < q < X^{1/2+\varepsilon}} \frac{1}{q^2} \sum_{n < X^{3\varepsilon}} d(n)S(h,n;q)I(n,q) + O(\frac{1}{\sqrt{X}}).$$

4.6 Averaging the Kloosterman Sums

In this part we state the lemmas that we will need in averaging the Kloosterman sums. These results were derived by an application of the Kuznetsov formula. The first lemma is due to Deshouillers and Iwaniec [48]. This will be used when we average the Kloosterman sums over all moduli.

Lemma 4.11. *Let $m \geq 1, P > 0, Q > 0$, and let $g(x,y)$ be a function of class C^4 with support on $[P,2P] \times [Q,2Q]$ satisfying*

$$\frac{\partial^{i+j}}{\partial q^i \partial r^j} g(x,y) \ll \frac{1}{P^i Q^j} \text{ for } 0 \leq i,j \leq 2. \tag{4.55}$$

Then for any complex numbers a_p we have

$$\sum_{P<p<2P}\sum_{Q<q<2Q} a_p g(p,q) S(h,\pm p,q) \ll (\sqrt{h}+Q)P^{1/2}h^{\theta}\Big(\sum_p |a_p|^2\Big)^{1/2}(hPQ)^{\varepsilon}. \quad (4.56)$$

The second lemma [6, Proposition 3.5.] is useful when the averaging over q is over multiples of an integer.

Lemma 4.12. *With the notation of Lemma 4.11 and for $N \in \mathbb{N}$ we have*

$$\sum_{\substack{P<p<2P}}\sum_{\substack{Q<q<2Q \\ N|q}} a_p g(p,q) S(h,\pm p,q) \qquad\qquad\qquad\qquad (4.57)$$

$$\ll Q\Big(\sum_p |a_p|^2\Big)^{1/2}\Big(1+\frac{hP}{Q^2}+\frac{P}{N}\Big)^{1/2}h^{\theta}\Big(1+\big(\frac{Q^2}{hP}\big)^{\theta}\Big)(hPQ)^{\varepsilon}.$$

4.7 Proof of Theorems

In this section we prove Theorems 4.1 and 4.2. We fix n, and we set $m - n = r$, therefore we have

$$\mathcal{E}_2(1,1) = \sum_{n<X^{3\varepsilon}}\sum_{X^{1/2-\varepsilon}<q<X^{1/2+\varepsilon}}\sum_{|r|<X^{3\varepsilon}}^{\infty} d(n+r)d(n)S(h,r;q)\frac{I(n+r,n,q)}{q^2}+O(\frac{1}{\sqrt{X}}).$$

Note that $I(n+r,n,q)$ is a function of q and r so we set $I(n+r,n,q) := I(q,r)$. An important part of the proof of theorems is to show that the functions that are attached to the Kloosterman sums satisfy (4.55). We will show this for the function $I(n+r,n,q)$. The other functions are similar to this case. In order to apply Lemma 4.11 we need to show that $I(q,r)/q^2$ oscillates mildly with respect to q,r.

Lemma 4.13. *Let $X^{1/2-\varepsilon} < Q < X^{1/2+\varepsilon}$ and $\mathcal{R} < X^{3\varepsilon}$. Then for $Q < q < 2Q$ and $\mathcal{R} < r < 2\mathcal{R}$ we have*

$$\frac{\partial^{i+j}}{\partial q^i \partial r^j}\Big(\frac{1}{X^{136\varepsilon}}\frac{I(q,r)}{q^2}\Big) \ll \frac{1}{Q^i \mathcal{R}^j}.$$

Proof. By (4.51) it follows that

$$\frac{\partial}{\partial q}\frac{I(q,r)}{q^2} \asymp \frac{1}{n(n+r)}\int_0^\infty\int_0^\infty uY_0(u)vY_0(v)\frac{\partial}{\partial q}q^2E\left(\frac{u^2q^2}{(4\pi)^2(n+r)},\frac{v^2q^2}{(4\pi)^2n},q\right)dudv. \quad (4.58)$$

By the chain rule for multi-variable functions

$$\frac{\partial}{\partial q}q^2E = 2qE + \frac{2q^3u^2}{(4\pi)^2(n+r)}E^{(1,0,0)} + \frac{2q^3v^2}{(4\pi)^2n}E^{(0,1,0)} + q^2E^{(0,0,1)}. \quad (4.59)$$

Considering the range of q in Lemma, we use these bounds $E < 1/X$, $E^{(1,0,0)} < 1/X^2$ and $E^{(0,1,0)} < 1/X^2$. For $E^{(0,0,1)}$ we need to estimate

$$\frac{\partial}{\partial q}\Delta_q(x-y-h) = \sum_{r=1}^\infty\frac{\partial}{\partial q}\left(\frac{w(qr)-w(\frac{x-y-h}{qr})}{qr}\right) = -\frac{\Delta_q(x-y-h)}{q}$$

$$+\sum_r\frac{w'(qr)}{q} + \frac{(x-y-h)w'(x-y-h/qr)}{q^3r^2}. \quad (4.60)$$

By Lemma 2 in [22] we have $w^i(u) \ll \frac{1}{Q^{i+1}}$, and $\Delta_q(u) \ll \frac{1}{qQ}$. Therefore, each term in (4.60) is bounded by $\frac{1}{qQ^2}$. Plugging in these bounds into (4.59) and considering the range of q we have

$$\frac{\partial}{\partial q}q^2E \ll (1+u^2+v^2)\frac{X^{3\varepsilon}}{\sqrt{X}}.$$

We use the above in (4.58) and by taking to account that since $X < \frac{u^2q^2}{(4\pi)^2(n+r)} < 2X$ the range in the integral for u,v is $0 < u,v < X^{5\varepsilon}$, we have

$$\frac{\partial}{\partial q}\frac{I(q,r)}{q^2} \ll \frac{X^{34\varepsilon}}{X^{\frac{1}{2}+\varepsilon}} \ll \frac{1}{Q^{1-\varepsilon}}.$$

For the second derivative with respect to q we apply the same method to each term in (4.59) and use the similar bound on the derivatives of E. For the derivatives with respect to r we

97

have

$$\frac{\partial}{\partial r}\frac{I(q,r)}{q^2} = \frac{4\pi^2}{(4\pi)^4 n(n+r)}\int_0^\infty\int_0^\infty uY_0(u)vY_0(v)\frac{\partial}{\partial r}q^2E(\frac{u^2q^2}{(4\pi)^2(n+r)},\frac{v^2q^2}{(4\pi)^2n},q)dudv.$$

Also we have

$$\left|\frac{\partial}{\partial r}q^2E(\frac{u^2q^2}{(4\pi)^2(n+r)},\frac{v^2q^2}{(4\pi)^2n},q)\right| = \left|\frac{u^2q^4}{(4\pi)^2(n+r)^2}E^{(1,0,0)}\right| \ll \frac{u^2X^{4\varepsilon}}{r^2},$$

and therefore

$$\frac{\partial}{\partial r}\frac{I(q,r)}{q^2} \ll \frac{X^{34\varepsilon}}{\mathcal{R}^2}.$$

A similar calculation we use for second derivative in respect to r and derivative in respect to q, r. This finishes the proof of Lemma. □

Now we need to apply Lemma 4.11 to $X^{-136\varepsilon}I(q,r)q^{-2}$. In order to do that we need to put the support of the function in dyadic intervals. Here we use Harcos's treatment [32]. Let ρ be a smooth function whose support lies in $[1,2]$ and satisfies the following identity for $x > 0$:

$$\sum_{k=-\infty}^{\infty}\rho(2^{-k/2}x) = 1. \tag{4.61}$$

We write

$$\frac{1}{X^{136\varepsilon}}\frac{I(q,r)}{q^2} = \sum_{k,l=-\infty}^{\infty}I_{k,l}(q,r),$$

where

$$I_{k,l}(q,r) = \frac{1}{X^{136\varepsilon}}\frac{I(q,r)}{q^2}\rho(\frac{q}{2^{k/2}Q})\rho(\frac{r}{2^{l/2}R})$$

and $Q = X^{1/2+\varepsilon}$ and $R = X^{3\varepsilon}$. The support of $I_{k,l}(q,r)$ is $[2^{k/2}Q, 2^{k/2+1}Q]\times[2^{l/2}R, 2^{l/2+1}R]$. Note that we just need to use Lemma 4.11 in the range of $X^{1/2-\varepsilon} < q < X^{1/2+\varepsilon}$ and $r < R$. Also For $r = 0$ the Kloosterman sum simplifies to the Ramanujan sum and therefore we estimate the corresponding error term trivially.

Proof of Theorem 4.1. Take $\varepsilon = \varepsilon/134$. We apply Lemma 4.11 to $I_{k,l}(q,r)$ for $-4\varepsilon\frac{\log X}{\log 2} \leq$

$k \leq 0$ and $-6\varepsilon \frac{\log X}{\log 2} \leq l \leq 0$. For the derivatives of $I_{k,l}(q,r)$ we need to have bounds on the derivatives of $\rho(\frac{q}{2^{k/2}Q})\rho(\frac{r}{2^{l/2}R})$ for which we have

$$\frac{\partial}{\partial q}\rho(\frac{q}{2^{k/2}Q})\rho(\frac{r}{2^{l/2}R}) \ll \frac{1}{2^{k/2}Q} \ll \frac{X^{4\varepsilon}}{Q} \tag{4.62}$$

The derivative with respect to r has a similar bound. Using Lemma 4.13 and the above we have that $I_{k,l}(q,r)$ satisfies the condition of Lemma 4.11. Therefore to have a upper bound on the error terms arising from (4.47), we apply Lemma 4.11 with $m = h$ and $P = R$ and $a_p = d(n)d(n+p)$ to $I_{k,l}(q,r)$. This will take care of the error term $\mathcal{E}_2(1,1)$. For the error terms $\mathcal{E}_1(1,1)$ we follow a similar method to show $I(n,q)$ in (4.49) oscillates mildly with respect to q and n. The only difference with $I(m,n,q)$ is that instead of one of the Bessel functions in (4.48) we have a $\log q$ term coming from $\lambda_{1,q}$. The derivative of $\log q$ has the desired decay with respect to q. This will finish the proof of theorem $\qquad \square$

Proof of Theorem 4.2. We give a sketch of the proof as it very similar to the proof of Theorem 4.1.

Main term. The main term here comes from Equations (4.43) and (4.44). We combine these with the argument of the section 6 of [22] and we have the main term is

$$\sum_{\substack{q<Q \\ (p,q)=1}} S(h,0;q)\frac{|\chi(q)|^2}{q^2}L(1,\chi)^2 \int_0^\infty f(x,x-h)\phi(h)dx \tag{4.63}$$

$$+ \sum_{\substack{q<Q \\ p|q}} S(h,0;q)\frac{\tau^2(\chi)}{q^2}L(1,\overline{\chi})^2 \int_0^\infty f(x,x-h)\phi(h)dx$$

Error term. The difference with the proof of Theorem 4.1 is that we split the sum over q in (4.43) and (4.44) into two cases: $(p,q) = 1$ and $p|q$. Recall that $h' = h/p$. For $(p,q) = 1$ we need to deal with averaging Kloosterman sums of the form $S(-h',-(n+m);q)$ over q

and m, n:

$$\sum_{\substack{q<Q \\ (p,q)=1}} \frac{1}{q^2} \left(\sum_{m,n=1}^{\infty} \tau_\chi(m)\overline{\tau_\chi(n)} S(-h', -(m+n); \ q) I_J(m,n,q) \right).$$

Note that $I_J(m,n,q)$ would be the same as $I(m,n,q)$ in Theorem 4.1 if we change Y_0 to J_0. For $p|q$ we average Kloosterman sums of the form $S(-h, -(n+m); \ q)$. For the sum over q with the condition $p|q$ we use Lemma 4.12 and we have the error term $O(X^{1/2+\theta+\varepsilon})$. For the sum over q with the condition $(p,q) = 1$, first we add the following terms

$$\sum_{\substack{q<Q \\ p|q}} \frac{1}{q^2} \left(\sum_{m,n=1}^{\infty} \tau_\chi(m)\overline{\tau_\chi(n)} S(-h', -(m+n); \ q) I_J(m,n,q) \right)$$

and then subtract them. By adding this we get a sum over all q, so we may use Lemma 4.11 and we get the error therm $O(X^{1/2+\varepsilon}h^\theta)$. For the terms that we had subtracted we use Lemma 4.12 and we get the error term $O(X^{1/2+\theta+\varepsilon})$. The final error is $O(X^{1/2+\theta+\varepsilon})$ as in (4.8). This finishes the proof of the first part of the Theorem.

Now to show the second part of the theorem regarding the sum of two squares note that the main term in this case is the same as (4.63) when we set $q = 4$. For the error term the proof is also very close to the proof of of (4.8), with only minor modification. Here the sum over q is divided to three cases: $(q,4) = 1$, $4|q$ and $q \equiv 2 \pmod 4$ and each involves a Kloosterman sums with different arguments. For $(q,4) = 1$, we add the sums over even q's and subtract them. We use Lemmas 4.11 and 4.12 respectively. The error term is $O(X^{1/2+\theta+\varepsilon})$. For $4|q$ we use Lemma 4.12 and the error term is $O(X^{1/2+\theta+\varepsilon})$. Finally for $q \equiv 2 \pmod 4$, we add the sums over q's such that $4|q$ and subtract them. We use Lemma 4.12 twice, once with sum over even q's and once with the sum over q's such that $4|q$. This finishes the proof of the Theorem. $\qquad\square$

4.8 Quadratic divisor problem

In this section we use a version of Dirichlet's hyperbola method to write the divisor function $d(n)$ in terms of a summation of a weight function. Our analysis of the left hand side of (4.16) follows the argument in [7]. Let ω be a smooth function such that $\omega(x) = 1$ on $[0,1]$ and $\omega(x) = 0$ on $[2,\infty)$. For $n < Q$ we have

$$d(n) = \sum_{\delta \mid n} \omega\left(\frac{\delta}{\sqrt{Q}}\right)\left(2 - \omega\left(\frac{n}{\delta\sqrt{Q}}\right)\right). \tag{4.64}$$

Thus

$$\sum_{am-n=h} d(m)d(n)f(am,n) = \sum_{m=1}^{\infty} d(m)d(am-h)f(am,am-h)$$

$$= \sum_{\delta=1}^{\infty} \omega\left(\frac{\delta}{\sqrt{Q}}\right)\sum_{\delta \mid n} d(am-h)f(am,am-h)\left(2 - \omega\left(\frac{m}{\delta\sqrt{Q}}\right)\right)$$

$$= \sum_{\delta=1}^{\infty} \omega\left(\frac{\delta}{\sqrt{Q}}\right)\sum_{n \equiv -h(a\delta)} d(n)f(n-h,n)\left(2 - \omega\left(\frac{n+h}{a\delta\sqrt{Q}}\right)\right)$$

Using Corollary 4.12. of [46] for the innermost sum we have

$$\sum_{am-n=h} d(m)d(n)f(am,n) = \sum_{q=1}^{\infty} \frac{(a,q)S(h,0;q)}{q^2}\int_0^\infty \left(\log\left(\frac{x}{q^2}\right) + 2\lambda\right)K_{(a,q),q}(x)f(ax,ax-h)dx$$

$$- 2\pi\sum_{q=1}^{\infty}\frac{(a,q)}{q^2}\sum_{n=1}^{\infty}d(n)S(h,n;q)\int_0^\infty Y_0\left(\frac{4\pi\sqrt{n(ax-h)}}{q}\right)K_{(a,q),q}(x)f(ax,ax-h)dx \quad (4.65)$$

$$- 2\pi\sum_{q=1}^{\infty}\frac{(a,q)}{q^2}\sum_{n=1}^{\infty}d(n)S(h,n;q)\int_0^\infty K_0\left(\frac{4\pi\sqrt{n(ax-h)}}{q}\right)K_{(a,q),q}(x)f(ax,ax-h)dx$$

where

$$K_{r,q}(x) = \sum_{\delta}\frac{1}{\delta}\omega\left(\frac{q\delta}{r\sqrt{Q}}\right)\left(2 - \omega\left(\frac{rx}{\delta q\sqrt{Q}}\right)\right).$$

Note that here since the support of f is $[X,2X] \times [X,2X]$, we can take $Q = 2X/a$, also using the definition we have that $K_{r,q}(x) = 0$ for $q > 2r\sqrt{Q}$. Similar to the proof of Theorem 4.1 we need to show that the functions attached to the Kloosterman sums in (4.65) oscillate

mildly with respect with q and n. In order to do this there is a minor difficulty in dealing with the function $K_{(a,q),q}(x)$ when (a,q) varies. Therefore we need to average over q's such that (a,q) is fixed. As in the case of the binary divisor problem we will show that the contribution from small q's is negligible. The integral in the second sum in (4.65) equals

$$\frac{1}{a} \int_0^\infty Y_0\left(\frac{4\pi\sqrt{n(x-h)}}{q}\right) K_{(a,q),q}\left(\frac{x}{a}\right) f(x, x-h)dx, \tag{4.66}$$

by the variable change $ax \to x$. In order to prove our result we need to estimate the second and third sum in (4.65). Using (4.66) we have that the second sum in (4.65) equals

$$\Theta := \sum_{q=1}^\infty \frac{(a,q)}{aq^2} \sum_{n=1}^\infty d(n)S(h,n;q) \int_0^\infty Y_0\left(\frac{4\pi\sqrt{n(x-h)}}{q}\right) K_{(a,q),q}\left(\frac{x}{a}\right) f(x, x-h)dx \tag{4.67}$$

For the rest of the paper we focus on estimating this sum since the third sum in (4.65) shall satisfy the same bound and can be handled similarly. Let $(a,q) = d$, this condition is equivalent to $(a/d, q/d) = 1$ and we detect this with $\sum_{\sigma|(\frac{a}{d},\frac{q}{d})} \mu(\sigma)$. Using this the outer sum in (4.67) simplifies to

$$\sum_{\substack{d|a}} \sum_{\substack{q \\ (a,q)=d}} = \sum_{d|a} \sum_{\sigma|\frac{a}{d}} \mu(\sigma) \sum_{\substack{q \\ \sigma d|q}} \tag{4.68}$$

and hence

$$\Theta = \sum_{d|a} \sum_{\sigma|\frac{a}{d}} \mu(\sigma) \sum_{\substack{q \\ \sigma d|q}} \Theta_{a,h}(\sigma), \tag{4.69}$$

where

$$\Theta_{a,h}(\sigma) = \frac{d}{a} \sum_{\substack{q=1 \\ \sigma d|q}}^\infty \frac{1}{q^2} \sum_{n=1}^\infty d(n)S(h,n;q)I(n,q,d), \tag{4.70}$$

and

$$I(n,q,d) := \int_0^\infty -2\pi Y_0\left(\frac{4\pi\sqrt{n(x-h)}}{q}\right) K_{d,q}(x/a) f(x, x-h)dx. \tag{4.71}$$

Our aim is to show that

$$\Theta_{a,h}(\sigma) \ll \frac{d}{a} X^{1/2+\theta}. \tag{4.72}$$

Putting this in (4.69) gives

$$\Theta \ll X^{1/2+\theta} \sum_{d|a} \frac{2^{\omega(a/d)}d}{a} \ll X^{1/2+\theta+\varepsilon}. \tag{4.73}$$

and this establishes Theorem 4.3. In order to prove (4.72) we will divide the range of the summation over n, q to three cases:

1. $q < X^{1/2-\varepsilon}$ and $n \geq 1$.

2. $X^{1/2-\varepsilon} \leq q \leq \sqrt{aX}$ and $n \gg q^2/X^{1-3\varepsilon}$.

3. $X^{1/2-\varepsilon} \leq q \leq \sqrt{aX}$ and $n \ll q^2/X^{1-3\varepsilon}$.

We estimate cases 1, 2, by using Lemmas 4.14 and 4.15 and the trivial bound for the Kloosterman sum. For case 3 we apply Lemma 4.12. To proceed we prove the following Lemmas for $I(n, q, d)$ to show that the contribution of small q's are negligible

Lemma 4.14. *For $q < X^{1/2-\varepsilon}$, we have that*

$$I(n, q, d) \ll n^{-2}X^{-1}.$$

Proof. First we set

$$F(x) = K_{d,q}(x/a)f(x, x-h).$$

By the product and multi variable chain rule, equation (4.6) for derivatives of f and [7, Equation (2.30)] i.e.

$$\frac{\partial^{i+j}}{\partial x^i \partial q^j} K_{r,q}(x) \ll_{i,j} \frac{\log Q}{X^i q^j}, \tag{4.74}$$

for derivatives of K we have that

$$F^{(i)}(x) \ll \frac{1}{x^i}.$$

103

Recall that the support of F is $[X, 2X]$. By the variable change $u = 4\pi\sqrt{n(x-h)}/q$ and integration by parts i times using the recursive formula we have

$$I(n,q,d) \asymp \frac{q^{2(i+1)}}{n^{i+1}} \int_0^\infty u^{i+1} Y_i(u) F^{(i)}\left(\frac{u^2 q^2}{n(4\pi)^2} + h\right) du. \tag{4.75}$$

we switch back u to x in the above and we have

$$I(n,q,d) \asymp \frac{q^{2(i+1)}}{n^{i+1}} \int_0^\infty \left(\frac{4\pi\sqrt{n(x-h)}}{q}\right)^{i+1} Y_i\left(\frac{4\pi\sqrt{n(x-h)}}{q}\right) F^{(i)}(x) \frac{\sqrt{n}}{q\sqrt{(x-h)}} dx$$

$$\asymp \frac{q^i}{n^{i/2}} \int_0^\infty (x-h)^{\frac{i}{2}} Y_i\left(\frac{4\pi\sqrt{n(x-h)}}{q}\right) F^{(i)}(x) dx.$$

We use

$$F^{(i)}(x) \ll \frac{1}{X^i}, \quad Y_i(u) \ll 1 \quad \text{and} \quad (x-h) \ll X,$$

on the above and by considering the fact that the support of F is $[X, 2X]$ we have

$$I(n,q,d) \ll \frac{q^i}{n^i X^{i/2-1}}. \tag{4.76}$$

Now, by using the fact that $q < X^{1/2-\varepsilon}$ and i large enough, we conclude the proof. $\qquad\square$

Lemma 4.15. *Let* $Q > X^{1/2-\varepsilon}$. *Then for* $q \in [Q, 2Q]$, *we have that*

$$\sum_{n > Q^2/X^{1-3\varepsilon}} d(n)|I(n,q,d)| \ll 1. \tag{4.77}$$

Proof. By using (4.76) we have

$$\sum_{n > Q^2/X^{1-3\varepsilon}} d(n)|I(n,q,d)| \ll \frac{q^i}{X^{\frac{i}{2}-1}} \sum_{n > Q^2/X^{1-3\varepsilon}} \frac{d(n)}{n^{\frac{i}{2}}}$$

$$\ll \frac{q^i}{X^{\frac{i}{2}-1}} \left(\frac{Q^2}{X^{1-3\varepsilon}}\right)^{-\frac{i}{2}+1+\varepsilon} \ll \frac{Q^2}{X^{\frac{3}{2}(i-6)\varepsilon}}.$$

Now similar to the proof of Lemma 4.14 by taking i large enough we obtain (4.77). $\qquad\square$

This lemma shows that we only need to consider the contribution of $n < Q^2/X^{1-3\varepsilon}$ in (4.70). Now we need to show that the derivatives of $I(n,q,d)/q^2$, satisfy the conditions of Lemma 4.12. Note that by using a smooth partition of unity similar to the proof of Theorem 4.1 we break the support of $I(n,q,d)$ to dyadic intervals. The largest error term comes from $d\sqrt{2X/a} < q < 2d\sqrt{X/a}$, and $d^2X^\varepsilon a^{-1} < n < 2d^2X^\varepsilon a^{-1}$. Also $K_{d,q} = 0$ for $q > 2d\sqrt{X/a}$.

Lemma 4.16. *Let $Q > X^{1/2-\varepsilon}$ and $q \in [Q, 2Q]$, and $n \in [N, 2N]$ then for $0 \le i, j \le 2$*

$$\frac{\partial^{i+j}}{\partial q^i \partial n^j}\left(\frac{Q^{2-\varepsilon}}{X}\frac{I(n,q,d)}{q^2}\right) \ll_{i,j} \frac{1}{Q^i N^j}. \tag{4.78}$$

Proof. We differentiate once with respect to q and once with respect to n. We state the necessary bounds on functions in the integrand (4.71). The derivative with respect to n is

$$\frac{\partial}{\partial n}I(n,q,d) = \int_0^\infty -\frac{1}{nq^2}\frac{4\pi^2\sqrt{n(x-h)}}{q}Y_0'\left(\frac{4\pi\sqrt{n(x-h)}}{q}\right)K_{d,q}(x/a)f(x,x-h)dx \tag{4.79}$$

By Lemma 4.15 we may assume $n \le q^2/x^{1-3\varepsilon}$. Therefore for $z = 4\pi\sqrt{n(x-h)}/q$, since $x \in [X, 2X]$ we have $z \ll X^\varepsilon$. In order to use (4.25) we need to multiply the integral (4.79) with $1/(1+z)$ and since $z \ll X^\varepsilon$ this would at most augment it by X^ε. Now we pull out $1/n$ from (4.79) and we use $q \in [Q, 2Q]$, and the fact that f is supported in $[X, 2X] \times [X, 2X]$ and $K \ll \log X$ to get (4.78) for $(i=0, j=1)$. If we differentiate $I(n,q,d)$ with respect to q using (4.74) we obtain (4.78) for $(i=1, j=0)$ exactly similar to the case $(i=0, j=1)$. Now we differentiate (4.79) with respect to q to obtain (4.78) for $(i=1, j=1)$.

$$\frac{\partial}{\partial q \partial n}I(n,q,d) = \frac{1}{n}\int_0^\infty -\frac{\partial}{\partial q}\left(\frac{1}{q^2}\frac{4\pi^2\sqrt{(x-h)}}{q}Y_0'\left(\frac{4\pi\sqrt{n(x-h)}}{q}\right)K_{d,q}(x/a)f(x,x-h)dx\right).$$

All the terms with q in the denominator and also $K_{d,q}$ would obviously give us the $1/q$ saving that we need. We just treat the term with derivative of Bessel function.

$$\frac{\partial}{\partial q}Y_0'\left(\frac{4\pi\sqrt{n(x-h)}}{q}\right) = \frac{1}{q}\left(\frac{-4\pi\sqrt{n(x-h)}}{q}Y_0^{(2)}\left(\frac{4\pi\sqrt{n(x-h)}}{q}\right)\right),$$

which for bounding this we use (4.25) and the fact that $z \ll X^\varepsilon$. For the cases $(i = 2, j = 1)$, $(i = 1, j = 2)$ and $(i = 2, j = 2)$ the proof is similar to the case $(i = 1, j = 1)$. This finishes the proof of the Lemma. $\qquad\square$

Proof of Theorem 4.3. As mentioned earlier we need to establish (4.72). Here the main term is:

$$\sum_{q=1}^{\infty} \frac{(a,q)S(h,0;q)}{q^2} \int_0^{\infty} \left(\log\left(\frac{x}{q^2}\right) + 2\lambda \right) K_{(a,q),q}(x) f(ax, ax - h) dx \tag{4.80}$$

For the error term, note that to use Lemma 4.12 we need to use the smooth partition of unity to put the support of $I(n,q,d)/q^2$ in dyadic intervals. In order to do this let ρ be the same as the proof of Theorem 4.1 and ρ satisfies (4.61) and $R = d\sqrt{2X/a}$ and $S = d^2 X^\varepsilon/a$, we write $q^{-2}I(n,q,d) = \sum_{k,l=-\infty}^{\infty} I_{k,l}(n,q,d)$, where

$$I_{k,l}(n,q,d) = q^{-2}I(n,q,d)\rho\left(\frac{q}{2^{k/2}R}\right)\rho\left(\frac{n}{2^{l/2}S}\right). \tag{4.81}$$

Thus we have

$$\Theta_{a,h}(\sigma) = \sum_{k,l} \frac{d}{a} \sum_{\substack{q=1 \\ \sigma d | q}}^{\infty} \frac{1}{q^2} \sum_{n=1}^{\infty} d(n)S(h,n;q)I_{k,l}(n,q,d). \tag{4.82}$$

The support of $I_{k,l}$ is $[2^{k/2}R, 2^{k/2+1}R] \times [2^{l/2}S, 2^{l/2+1}S]$. Now since $K_{d,q} = 0$ for $q > 2d\sqrt{X/a}$ and the fact that $I_{k,l}$ is supported on $2^{k/2}d\sqrt{2X/a} \le q \le 2^{k/2+1} d\sqrt{2X/a}$, we conclude that $k \le 0$. Also we have $|k| \ll \log X$. To continue with the proof we are returning to our range separation for the summation over q, n in (4.70):

1. $q < X^{1/2-\varepsilon}$ and $n \ge 1$. For this range using Lemma 4.14 we have $I_{k,l}(n,q,d) \ll$

$I(n,q,d) \ll n^{-2}X^{-1}$ and consequently

$$\sum_{\substack{q=1 \\ d\sigma|q}}^{X^{1/2-\varepsilon}} \sum_{k,l} \sum_{n=1}^{\infty} d(n)\frac{I_{k,l}(n,q,d)}{q^2} S(h,n;q)$$

$$\ll \sum_{\substack{q=1 \\ d\sigma|q}}^{X^{1/2-\varepsilon}} \sum_{n=1}^{\infty} d(n)\frac{I(n,q,d)}{q^2} S(h,n;q) \ll \frac{1}{X}\sum_{\substack{q=1 \\ d\sigma|q}}^{X^{1/2-\varepsilon}} \sum_{n=1}^{\infty} \frac{d(n)}{qn^2} \ll X^{\varepsilon-1}.$$

2. $X^{1/2-\varepsilon} \leq q \leq d(X/a)^{1/2}$ and $n \gg q^2 X^{3\varepsilon-1}$. First note that if $d/\sqrt{a} < X^{-\varepsilon}$ then since $K_{d,q} = 0$ for $q > 2d(X/a)^{1/2}$, we fall into the first range. Now by using Lemma 4.15 we have

$$\sum_{k,l} \sum_{\substack{X^{1/2-\varepsilon} \leq q \leq d(X/a)^{1/2} \\ d\sigma|q}} \sum_{n\gg q^2 X^{3\varepsilon-1}} d(n)\frac{I_{k,l}(n,q,d)}{q^2} S(h,n;q)$$

$$= \sum_{\substack{X^{1/2-\varepsilon} \leq q \leq d(X/a)^{1/2} \\ d\sigma|q}} \sum_{n\gg q^2 X^{3\varepsilon-1}} d(n)\frac{I(n,q,d)}{q^2} S(h,n;q) \ll \sum_{X^{1/2-\varepsilon} \leq q \leq d(X/a)^{1/2}} \frac{1}{q} \ll 1.$$

3. $X^{1/2-\varepsilon} \leq q \leq \sqrt{aX}$ and $n \ll q^2 X^{3\varepsilon-1}$. For this range we need to apply Lemma 4.12. By using (4.81) we beak the support of I into dyadic intervals and for the current range we have to deal with $I_{k,l}$ where

$$\frac{2}{\log 2}\Big(\log\Big(\frac{\sqrt{a}}{\sqrt{2}dX^\varepsilon}\Big) - 1\Big) \leq k \leq 0.$$

and

$$\frac{2}{\log 2}\log\Big(\frac{a}{d^2 X^\varepsilon}\Big) \leq l \leq \frac{2}{\log 2}\log\Big(\frac{d^2 q^2}{aX^{1-2\varepsilon}}\Big) - 3.$$

Our aim is to handled the following sum for k,l in the above range

$$\sum_{\substack{k,l \\ d\sigma|q}} \sum_{q=1}^{\infty} \sum_{n=1}^{\infty} d(n)\frac{I_{k,l}(n,q,d)}{q^2} S(h,n;q)$$

Each of the $I_{k,l}$ in the above range can be handled using Lemma 4.12. Here we only consider the range $R < q < 2R$, and $S < n < 2S$ i.e $k = l = 1$, for which we have the biggest error term. Now since the volume of the box that k, l take their values in, is bounded by $(\log X)^2$ we have the final error term is bounded by $(\log X)^2$ times the error that comes from $k = l = 1$. Lemma 4.16 enable us to average the Kloosterman sums above by employing Lemma 4.12 and also save a factor $X/Q^{2-\varepsilon}$. Thus by setting $a_p = d(p)$, $Q = R$ and $P = S$ in Lemma 4.16 we have the above is bounded by

$$\frac{a}{d^2} d \left(\frac{X}{a}\right)^{1/2} \left(\frac{d^2}{a}\right)^{1/2} \left(1 + \frac{h}{X} + \frac{d}{a\sigma}\right)^{1/2} h^\theta \left(1 + \left(\frac{X}{h}\right)^\theta\right)$$

and therefore (4.70) is bounded by $dX^{1/2+\theta+\varepsilon}/a$. This finishes the proof of (4.72) and using (4.73) finishes the proof of the theorem.

$\square$

Bibliography

[1] F. Aryan. Incomplete kloosterman suml. *Math Overflow question (2014), http://mathoverflow.net/questions/175822/incomplete-kloosterman-sum.*

[2] F. Aryan. On binary and quadratic divisor problems. *arXiv:1502.06067v1* .

[3] Farzad Aryan. The distribution of *k*-tuples of reduced residues. *Mathematika*, 61(1):72–88, 2015.

[4] Farzad Aryan. Distribution of Squares Modulo a Composite Number. *Int. Math. Res. Not. IMRN*, (23):12405–12431, 2015.

[5] R. Balasubramanian, J. B. Conrey, and D. R. Heath-Brown. Asymptotic mean square of the product of the Riemann zeta-function and a Dirichlet polynomial. *J. Reine Angew. Math.*, 357:161–181, 1985.

[6] Valentin Blomer. Shifted convolution sums and subconvexity bounds for automorphic *L*-functions. *Int. Math. Res. Not.*, (73):3905–3926, 2004.

[7] Valentin Blomer, Gergely Harcos, and Philippe Michel. Bounds for modular *L*-functions in the level aspect. *Ann. Sci. École Norm. Sup. (4)*, 40(5):697–740, 2007.

[8] H. M. Bui, M. B. Milinovich, and N. C. Ng. A note on the gaps between consecutive zeros of the Riemann zeta-function. *Proc. Amer. Math. Soc.*, 138(12):4167–4175, 2010.

[9] D. A. Burgess. The distribution of quadratic residues and non-residues. *Mathematika*, 4:106–112, 1957.

[10] Fernando Chamizo. Correlated sums of $r(n)$. *J. Math. Soc. Japan*, 51(1):237–252, 1999.

[11] S. Chowla. *The Riemann hypothesis and Hilbert's tenth problem.* Mathematics and Its Applications, Vol. 4. Gordon and Breach Science Publishers, New York-London-Paris, 1965.

[12] J. B. Conrey, A. Ghosh, and S. M. Gonek. A note on gaps between zeros of the zeta function. *Bull. London Math. Soc.*, 16(4):421–424, 1984.

[13] J. B. Conrey and S. M. Gonek. High moments of the Riemann zeta-function. *Duke Math. J.*, 107(3):577–604, 2001.

[14] Harald Cramr. On the order of magnitude of the difference between consecutive prime numbers. *Acta Arithmetica*, 2(1):23–46, 1936.

[15] H. Davenport. On the Distribution of Quadratic Residues (mod p). *J. London Math. Soc.*, S1-8(1):46.

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

[17] J.-M. Deshouillers and H. Iwaniec. An additive divisor problem. *J. London Math. Soc. (2)*, 26(1):1–14, 1982.

[18] J.-M. Deshouillers and H. Iwaniec. Kloosterman sums and Fourier coefficients of cusp forms. *Invent. Math.*, 70(2):219–288, 1982/83.

[19] W. Duke, J. Friedlander, and H. Iwaniec. Bounds for automorphic *L*-functions. *Invent. Math.*, 112(1):1–8, 1993.

[20] W. Duke, J. Friedlander, and H. Iwaniec. Erratum: "Bounds for automorphic *L*-functions. II" [Invent. Math. **115** (1994), no. 2, 219–239; MR1258904 (95a:11044)]. *Invent. Math.*, 140(1):227–242, 2000.

[21] W. Duke, J. B. Friedlander, and H. Iwaniec. Bounds for automorphic *L*-functions. II. *Invent. Math.*, 115(2):219–239, 1994.

[22] W. Duke, J. B. Friedlander, and H. Iwaniec. A quadratic divisor problem. *Invent. Math.*, 115(2):209–217, 1994.

[23] P. Erdös. The difference of consecutive primes. *Duke Math. J.*, 6:438–441, 1940.

[24] Theodor Estermann. Berichtigung zu meiner Arbeit "Über die Darstellungen einer Zahl als Differenz von zwei Produkten". *J. Reine Angew. Math.*, 166:64, 1932.

[25] Shaoji Feng and Xiaosheng Wu. On gaps between zeros of the Riemann zeta-function. *J. Number Theory*, 132(7):1385–1397, 2012.

[26] John B. Friedlander and Henryk Iwaniec. Incomplete Kloosterman sums and a divisor problem. *Ann. of Math. (2)*, 121(2):319–350, 1985. With an appendix by Bryan J. Birch and Enrico Bombieri.

[27] Roger Godement and Hervé Jacquet. *Zeta functions of simple algebras*. Lecture Notes in Mathematics, Vol. 260. Springer-Verlag, Berlin-New York, 1972.

[28] D. A. Goldston and S. M. Gonek. Mean value theorems for long Dirichlet polynomials and tails of Dirichlet series. *Acta Arith.*, 84(2):155–192, 1998.

[29] Andrew Granville and Pär Kurlberg. Poisson statistics via the Chinese remainder theorem. *Adv. Math.*, 218(6):2013–2042, 2008.

[30] Ben Green. On a variant of the large sieve. *preprint available at arXiv:0807.5037*.

[31] Ben Green and Adam J. Harper. Inverse questions for the large sieve. *Geom. Funct. Anal.*, 24(4):1167–1203, 2014.

[32] Gergely Harcos. An additive problem in the Fourier coefficients of cusp forms. *Math. Ann.*, 326(2):347–365, 2003.

[33] Miriam Hausman and Harold N. Shapiro. On the mean square distribution of primitive roots of unity. *Comm. Pure Appl. Math.*, 26:539–547, 1973.

[34] Winston Heap. The twisted second moment of the Dedekind zeta function of a quadratic field. *Int. J. Number Theory*, 10(1):235–281, 2014.

[35] D. R. Heath-Brown. The fourth power moment of the Riemann zeta function. *Proc. London Math. Soc. (3)*, 38(3):385–422, 1979.

[36] D. R. Heath-Brown. The divisor function $d_3(n)$ in arithmetic progressions. *Acta Arith.*, 47(1):29–56, 1986.

[37] D. R. Heath-Brown. Arithmetic applications of Kloosterman sums. *Nieuw Arch. Wiskd. (5)*, 1(4):380–384, 2000.

[38] H. A. Helfgott and A. Venkatesh. How small must ill-distributed sets be? In *Analytic number theory*, pages 224–234. Cambridge Univ. Press, Cambridge, 2009.

[39] C. Hooley. An asymptotic formula in the theory of numbers. *Proc. London Math. Soc. (3)*, 7:396–413, 1957.

[40] C. Hooley. On the difference of consecutive numbers prime to n. *Acta Arith.*, 8:343–347, 1962/1963.

[41] Christopher Hooley. On the difference between consecutive numbers prime to n. II. *Publ. Math. Debrecen*, 12:39–49, 1965.

[42] Christopher Hooley. On the difference between consecutive numbers prime to n. III. *Math. Z.*, 90:355–364, 1965.

[43] Aleksandar Ivić. The general additive divisor problem and moments of the zeta-function. In *New trends in probability and statistics, Vol. 4 (Palanga, 1996)*, pages 69–89. VSP, Utrecht, 1997.

[44] Aleksandar Ivić. On the ternary additive divisor problem and the sixth moment of the zeta-function. In *Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995)*, volume 237 of *London Math. Soc. Lecture Note Ser.*, pages 205–243. Cambridge Univ. Press, Cambridge, 1997.

[45] Henryk Iwaniec. *Spectral methods of automorphic forms*, volume 53 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI; Revista Matemática Iberoamericana, Madrid, second edition, 2002.

[46] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[47] M. Jutila. *Lectures on a method in the theory of exponential sums*, volume 80 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*. Published for the Tata Institute of Fundamental Research, Bombay; by Springer-Verlag, Berlin, 1987.

[48] M. Jutila. A variant of the circle method. In *Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995)*, volume 237 of *London Math. Soc. Lecture Note Ser.*, pages 245–254. Cambridge Univ. Press, Cambridge, 1997.

[49] Henry H. Kim. Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2. *J. Amer. Math. Soc.*, 16(1):139–183, 2003. With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak.

[50] Henry H. Kim and Freydoon Shahidi. Cuspidality of symmetric powers with applications. *Duke Math. J.*, 112(1):177–197, 2002.

[51] E. Kowalski, P. Michel, and J. VanderKam. Rankin-Selberg L-functions in the level aspect. *Duke Math. J.*, 114(1):123–191, 2002.

[52] M. Kreh. Bessel functions, lecture notes. *Penn State-Gottingen Summer School on Number Theory*.

[53] Pär Kurlberg and Zeév Rudnick. The distribution of spacings between quadratic residues. *Duke Math. J.*, 100(2):211–242, 1999.

[54] Ju. V. Linnik. *The dispersion method in binary additive problems*. Translated by S. Schuur. American Mathematical Society, Providence, R.I., 1963.

[55] Tom Meurman. On the binary additive divisor problem. In *Number theory (Turku, 1999)*, pages 223–246. de Gruyter, Berlin, 2001.

[56] P. Michel. The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points. *Ann. of Math. (2)*, 160(1):185–236, 2004.

[57] H. L. Montgomery. The pair correlation of zeros of the zeta function. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 181–193. Amer. Math. Soc., Providence, R.I., 1973.

[58] H. L. Montgomery and A. M. Odlyzko. Gaps between zeros of the zeta function. In *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, volume 34 of *Colloq. Math. Soc. János Bolyai*, pages 1079–1106. North-Holland, Amsterdam, 1984.

[59] H. L. Montgomery and R. C. Vaughan. Hilbert's inequality. *J. London Math. Soc. (2)*, 8:73–82, 1974.

[60] H. L. Montgomery and R. C. Vaughan. On the distribution of reduced residues. *Ann. of Math. (2)*, 123(2):311–333, 1986.

[61] H. L. Montgomery and R. C. Vaughan. A basic inequality. In *Proceedings of the Congress on Number Theory (Spanish) (Zarauz, 1984)*, pages 163–175. Univ. País Vasco-Euskal Herriko Unib., Bilbao, 1989.

[62] Yōichi Motohashi. The binary additive divisor problem. *Ann. Sci. École Norm. Sup. (4)*, 27(5):529–572, 1994.

[63] Julia Mueller. On the difference between consecutive zeros of the Riemann zeta function. *J. Number Theory*, 14(3):327–331, 1982.

[64] Ritabrata Munshi. Shifted convolution sums for $GL(3) \times GL(2)$. *Duke Math. J.*, 162(13):2345–2362, 2013.

[65] Terence Tao. Small residue classes with small reciprocal. *Math Overow question (2011) available at http://mathoverflow.net/questions/69509/small-residue-classes-with-small-reciprocal.*

[66] A. I. Vinogradov. SL$_n$ techniques and the density conjecture. *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 168(Anal. Teor. Chisel i Teor. Funktsii. 9):5–10, 187, 1988.

[67] Georges Voronoi. Sur un problème du calcul des fonctions asymptotiques. *J. Reine Angew. Math.*, 126:241–282, 1903.

[68] André Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U. S. A.*, 34:204–207, 1948.