On certain exponential and character sums

Bryce Kerr

A thesis in fulfilment of the requirements for the degree of
Doctor of Philosophy

School of Mathematics and Statistics
Faculty of Science

March 2017

PLEASE TYPE

THE UNIVERSITY OF NEW SOUTH WALES
Thesis/Dissertation Sheet

Surname or Family name: Kerr

First name: Bryce Other name/s: Denis

Abbreviation for degree as given in the University calendar: PhD

School: Mathematics and Statistics Faculty: Science

Title: On certain exponential and character sums

Abstract 350 words maximum: (PLEASE TYPE)

This thesis considers four distinct problems in the area of exponential and character sums. The strategy used to approach each problem can be considered as falling roughly into what is known as Vinogradov's method. The problems considered are rational exponential sums over the divisor function, character sums over shifted primes, character sums mixed with the exponential of a polynomial and the fourth moment of character sums. For each problem we obtain new quantitative bounds for the relevant sums which either improve or extend existing results except for the case of rational exponential sums over the divisor function whose solution has not been considered before although has been posed by Shparlinski.

Declaration relating to disposition of project thesis/dissertation

I hereby grant to the University of New South Wales or its agents the right to archive and to make available my thesis or dissertation in whole or in part in the University libraries in all forms of media, now or here after known, subject to the provisions of the Copyright Act 1968. I retain all property rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

I also authorise University Microfilms to use the 350 word abstract of my thesis in Dissertation Abstracts International (this is applicable to doctoral theses only).

....

The University recognises that there may be exceptional circumstances requiring restrictions on copying or conditions on use. Requests for restriction for a period of up to 2 years must be made in writing. Requests for a longer period of restriction may be considered in exceptional circumstances and require the approval of the Dean of Graduate Research.

FOR OFFICE USE ONLY Date of completion of requirements for Award:

ORIGINALITY STATEMENT

'I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.'

Signed .....

Date .....

On certain exponential and character sums

Bryce Kerr

A thesis in fulfilment of the requirements for the degree of
Doctor of Philosophy

School of Mathematics and Statistics
Faculty of Science

November 2016

Contents

Chapter 1

Introduction

1.1 Introduction

The contents of this thesis are a sequence of four papers in the area of exponential and character sums. A typical problem in this area may be stated in the following way.

Problem 1.1. *Given an integer q, a sequence of integers $\mathcal{S}_N = \{s_n\}_{1\leq n\leq N}$ and a character Ψ_q of either the additive group of residues $\mathbb{Z}/q\mathbb{Z}$ or the multiplicative group of reduced residues $(\mathbb{Z}/q\mathbb{Z})^*$, for which $0 < \varepsilon < 1$ does there exist a bound of the form*

$$\left|\sum_{s\in\mathcal{S}_N} \Psi_q(s)\right| \leq \varepsilon N. \tag{1.1}$$

Developing techniques for bounding sums of the form (1.1) have a wide range of applications in number theory and are motivated by their arithmetic consequences. Often one has a fixed sequence $\mathcal{S} = \{s_n\}_{n=1}^{\infty}$ and wishes to obtain a bound of the form

$$\left|\sum_{s\in\mathcal{S}_N} \Psi_q(s)\right| \leq \varepsilon_{q,N}|\mathcal{S}_N|, \tag{1.2}$$

where $\mathcal{S}_N = \{s \in \mathcal{S} : 1 \leq s \leq N\}$ and $\varepsilon_{q,N} \to 0$ as both q and $N \to \infty$. In other instances the sequence $\mathcal{S} = \mathcal{S}_{q,N} = \{s_{n,q}\}_{1\leq n\leq N_q}$ varies with both q and N. Various techniques have been developed which may be applied to sums of the form (1.1) when $\mathcal{S}$ belongs to a very general class of sequences. The methods used in this thesis bear closest resemblance to the method of Vinogradov.

We attempt to describe the method of Vinogradov in its most general form as being comprised of three distinct stages. One first uses properties specific to the set $\mathcal{S}_N$ to bound

sums of the form (1.1) in terms of certain multilinear forms

$$\sum_{a_1 \in \mathcal{A}_1} \cdots \sum_{a_k \in \mathcal{A}_k} \alpha_1(a_1) \dots \alpha_k(a_k) \Psi_0(a_1, \dots, a_k). \tag{1.3}$$

This is usually done through a sieve, combinatorial decomposition or certain averaging. Once the sums (1.1) are brought into the form (1.3) one considers various applications of partitioning summation depending on values of the function $\Psi_0(a_1, \dots, a_k)$, the Hölder inequality and possibly some sort of Fourier expansion. These three strategies are applied with the aim of separating variables occurring in summation (1.3) to reduce the problem to bounding a number of mean values. The resulting mean values can usually be interpreted geometrically as the number of solutions to a system of equations, as moments of certain integrals or as complete sums over finite fields.

1.2 Illustration of Vinogradov's method

We illustrate the use of Vinogradov's method with a simplified version of an argument due to Heath-Brown [35] and is related to Dirichlet L-Functions.

For a real number $t > 0$ consider the character $\Psi_t(n) = n^{it}$ of the multiplicative group $\mathbb{R}^*$ and summation over an interval $\mathcal{I} = (N, 2N]$. Our sums (1.1) may be written

$$S = \sum_{N < n \leq 2N} n^{it}. \tag{1.4}$$

For small z, the intervals $(N - z, 2N - z]$ and $(N, 2N]$ approximate each other and hence we may approximate S by

$$\frac{1}{UV} \sum_{U < u \leq 2U} \sum_{V < v \leq 2V} \sum_{N < n \leq 2N} (n + uv)^{it},$$

provided UV is not too large.

Let

$$S' = \sum_{U < u \leq 2U} \sum_{V < v \leq 2V} \sum_{N < n \leq 2N} (n + uv)^{it}.$$

Since the function n^{it} is multiplicative on $\mathbb{N}$ we may bound

$$S' \leq \sum_{N < n \leq 2N} \sum_{U < u \leq 2U} \left| \sum_{V < v \leq 2V} \left(\frac{n}{u} + v \right)^{it} \right|.$$

Partitioning summation over n and u according to the value of n/u gives

$$S' \leq \sum_{\lambda \in \mathbb{Q}} I(\lambda) \left| \sum_{V < v \leq 2V} (\lambda + v)^{it} \right|,$$

where $I(\lambda)$ is defined by

$$I(\lambda) = |\{ \ N < n \leq 2N, \ U < u \leq 2U \ : \ n = \lambda u \ \}| \, .$$

If δ is small, we may approximate the sum

$$\sum_{V < v \leq 2V} (\lambda + v)^{it} \, ,$$

by the average

$$\frac{1}{2\delta} \sum_{V < v \leq 2V} \int_{\lambda - \delta}^{\lambda + \delta} (z + v)^{it} dz,$$

and hence approximate S' in terms of

$$\frac{1}{2\delta} \sum_{\lambda \in \mathbb{Q}} I(\lambda) \left| \int_{\lambda - \delta}^{\lambda + \delta} \sum_{V < v \leq 2V} (z + v)^{it} dz \right| .$$

Let

$$S'' = \sum_{\lambda \in \mathbb{Q}} I(\lambda) \left| \int_{\lambda - \delta}^{\lambda + \delta} \sum_{V < v \leq 2V} (z + v)^{it} dz \right| .$$

An application of the Cauchy-Schwarz inequality gives

$$(S'')^2 \leq \left(\sum_{\lambda \in \mathbb{Q}} I(\lambda) \right) \left(\sum_{\lambda \in \mathbb{Q}} I(\lambda) \left| \int_{\lambda - \delta}^{\lambda + \delta} \sum_{V < v \leq 2V} (z + v)^{it} dz \right|^2 \right) .$$

From a second application of the same inequality we get

$$(S'')^4 \leq \left(\sum_{\lambda \in \mathbb{Q}} I(\lambda) \right)^2 \left(\sum_{\lambda \in \mathbb{Q}} I(\lambda)^2 \right) \left(\sum_{\substack{\lambda \in \mathbb{Q} \\ I(\lambda) \neq 0}} \left| \int_{\lambda - \delta}^{\lambda + \delta} \sum_{V < v \leq 2V} (z + v)^{it} dz \right|^4 \right) .$$

By the Hölder inequality

$$\left| \int_{\lambda - \delta}^{\lambda + \delta} \sum_{V < v \leq 2V} (z + v)^{it} dz \right|^4 \leq (2\delta)^3 \int_{\lambda - \delta}^{\lambda + \delta} \left| \sum_{V < v \leq 2V} (z + v)^{it} \right|^4 dz,$$

so that letting

$$S''' = \left(\sum_{\lambda\in\mathbb{Q}} I(\lambda)\right)^2 \left(\sum_{\lambda\in\mathbb{Q}} I(\lambda)^2\right) \left(\sum_{\substack{\lambda\in\mathbb{Q}\\ I(\lambda)\neq 0}} \int_{\lambda-\delta}^{\lambda+\delta} \left|\sum_{V<v\leq 2V} (z+v)^{it}\right|^4 dz\right), \tag{1.5}$$

we have

$$(S'')^4 \leq (2\delta)^3 S'''.$$

For the first term on the right of (1.5), since the numbers $I(\lambda)$ partition the set

$$\{(n,u)\ ; N < n \leq 2N,\quad U < u \leq 2U\},$$

into disjoint subsets we get

$$\sum_{\lambda\in\mathbb{Q}} I(\lambda) \leq NU.$$

For the second term on the right of (1.5), we have

$$\sum_{\lambda\in\mathbb{Q}} I(\lambda)^2 = \left|\{\ (n_1,u_1,n_2,u_2)\ ;\ n_1u_2 = n_2u_1,\ N < n_i \leq 2N,\quad U < u_i \leq 2U\}\right|, \tag{1.6}$$

which may be bounded by fixing values of n_1 and u_2 in (1.6) then counting divisors of the product n_1u_2.

For the last term on the right of (1.5), we consider the set of $\lambda \in \mathbb{Q}$ such that $I(\lambda) \neq 0$ as a subset of the set of reduced fractions with denominator at most U and numerator at most N. This set is U^{-2} spaced which implies that for suitably chosen δ, the intervals

$$[\lambda-\delta, \lambda+\delta] \quad \text{with} \quad \lambda\in\mathbb{Q} \quad \text{and} \quad I(\lambda)\neq 0,$$

do not overlap and hence

$$\sum_{\substack{\lambda\in\mathbb{Q}\\ I(\lambda)\neq 0}} \int_{\lambda-\delta}^{\lambda+\delta} \left|\sum_{V<v\leq 2V} (z+v)^{it}\right|^4 dz \leq \int_{N/4U}^{4N/U} \left|\sum_{V<v\leq 2V} (z+v)^{it}\right|^4 dz.$$

To bound the mean value on the right, we interchange summation and integration to get

$$\int_{N/4U}^{4N/U} \left| \sum_{V<v\leq 2V} (z+v)^{it} \right|^4 dz \leq \sum_{\substack{V<v_i\leq 2V \\ 1\leq i\leq 4}} \left| \int_{N/4U}^{4N/U} \left(\frac{(z+v_1)(z+v_2)}{(z+v_3)(z+v_4)} \right)^{it} dz \right|.$$

For a fixed tuple (v_1, v_2, v_3, v_4) we may estimate the integral

$$\int_{N/4U}^{4N/U} \left(\frac{(z+v_1)(z+v_2)}{(z+v_3)(z+v_4)} \right)^{it} dz,$$

via stationary phase or by considering the following elementary argument.

Let

$$F(z) = \frac{(z+v_1)(z+v_2)}{(z+v_3)(z+v_4)}, \tag{1.7}$$

and define the sets $I_1(\varepsilon)$ and $I_2(\varepsilon)$ by

$$I_1(\varepsilon) = \left\{ \frac{N}{4U} \leq z \leq \frac{4N}{U} : |F'(z)| \leq \varepsilon \right\}, \quad I_2(\varepsilon) = \left\{ \frac{N}{4U} \leq z \leq \frac{4N}{U} : |F'(z)| > \varepsilon \right\}.$$

We have

$$\int_{N/4U}^{4N/U} \left(\frac{(z+v_1)(z+v_2)}{(z+v_3)(z+v_4)} \right)^{it} dz = S_1 + S_2,$$

where

$$S_1 = \int_{I_1(\varepsilon)} F(z)^{it} dz, \quad S_2 = \int_{I_2(\varepsilon)} e^{it\log(F(z))} dz.$$

Considering S_1, we have

$$|S_1| \leq \mu(I_1(\varepsilon)),$$

where μ denotes the Lebesgue measure. This allows one to estimate S_1 by a consideration of the zeros of the rational function $F'(z)$.

For S_2 we first note that $I_2(\varepsilon)$ splits as a union over disjoint intervals $I_1, \ldots, I_k$, so we may write

$$S_2 = \sum_{j=1}^{k} \int_{I_j} \left(\frac{F(z)}{tF'(z)} \right) \left(\frac{tF'(z)}{F(z)} e^{it\log(F(z))} \right) dz.$$

The above sum may be bounded by combining an integration by parts with the fact that $|F'(z)| > \varepsilon$ whenever $z \in I_j$.

1.3 Outline of Thesis

The following problems comprise the main four sections of this thesis.

1.3.1 Rational Exponential Sums Over the Divisor Function

For integers q and a with $(a, q) = 1$ we consider giving nontrivial bounds for the sums

$$\sum_{1 \le n \le N} e^{2\pi i a \tau(n)/q}, \tag{1.8}$$

where $\tau(n)$ counts the number of divisors of n. This problem does not seem to be considered before although has been posed by Shparlinski [64]. We consider two different approaches.

Our first approach involves a decomposition of integers based on their squarefree part and reduces bounding the sums (1.8) to bounding sums over multiplicative subgroups. This allows us to apply results of Bourgain [4] and Shkredov [62, 63] concerning such sums. Our second approach applies only for prime modulus and involves applying the Selberg-Delange method to the Dirichlet series

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

where χ is a multiplicative character $\mod p$.

1.3.2 Character Sums Over Shifted Primes

For integers q and a with $(a, q) = 1$ and a character χ of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^*$ we consider giving nontrivial bounds for the sums

$$\sum_{M \le n \le M+N} \Lambda(n)\chi(n + a),$$

where $\Lambda(n)$ is the Von Mangoldt function defined by

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

This problem has been considered by Karatsuba [43] for the case of prime q and for arbitrary q by Friedlander, Gong and Shparlinski [26] and Rakhmonov [56]. Our result improves on the strength of a bound of Rakhmonov [56] in the range $N \ge q^{5/6+o(1)}$.

1.3.3 Mixed Character Sums

Let q be an integer, χ a character of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^*$ and F a polynomial with real coefficients. We consider giving nontrivial bounds for a number of different sums consisting of terms involving both $\chi(n)$ and $e^{2\pi iF(n)}$. The simplest example of such sums being

$$\sum_{M\leq n\leq M+N} \chi(n)e^{2\pi iF(n)}.$$

These sums and their generalizations have been considered by Enflo [22], Chang [15], Heath-Brown and Pierce [38] and Pierce [53]. We extend some bounds of Heath-Brown and Pierce [38] and Pierce [53] in various directions and improve on a bound of Chang [15].

1.3.4 The Fourth Moment of Character Sums

For a prime number q, we consider giving nontrivial bounds for the fourth moment

$$\frac{1}{q-1}\sum_{\chi\neq\chi_0}\left|\sum_{M\leq n\leq M+n}\chi(n)\right|^4, \tag{1.9}$$

where the above sum is over all non principal characters of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^*$. The sum (1.9) is related to the distribution of solutions to the congruence

$$x_1x_2 \equiv x_3x_4 \mod q, \tag{1.10}$$

with each x_i lying in an interval I_i.

This problem has been considered by Ayyad, Cochrane and Zheng [1] and Garaev and Garcia [31]. We give new bounds concerning the distribution of solutions to the equation (1.10) and as a Corollary give new bounds for the sums (1.9) which improve on previous results by a power of a logarithm. Our techniques are based on Ayyad, Cochrane and Zheng [1], Garaev [29] and Garaev and Garcia [31].

1.4 Notation

We adopt the following standard notation common to all four sections of this thesis.

Given two expressions f and g depending on a number of parameters, we write

$$f \ll g \quad \text{and} \quad f = O(g),$$

to mean that there exists some absolute constant $C > 0$ such that

$$|f| \leq C|g|, \tag{1.11}$$

as the parameters approach some specified values. If there is no mention of the values which the parameters approach then we will mean as the parameters approach infinity. In a similar fashion we write

$$f = o(g),$$

when (1.11) holds for any $C > 0$ provided the parameters are sufficiently large.

Given a positive integer q, we use $\mathbb{Z}/q\mathbb{Z}$ to denote the additive group of residues mod q and $(\mathbb{Z}/q\mathbb{Z})^*$ to denote the multiplicative group of reduced residues mod q. We let $e_q(an)$ denote the character

$$e_q(an) = e^{2\pi ian/q},$$

of the group $\mathbb{Z}/q\mathbb{Z}$ which we assume to be extended to $\mathbb{Z}$ by first identifying $Z/q\mathbb{Z}$ with the set $[0, 1, \ldots, q-1]$ and defining

$$e_q(an) = e_q(ab) \quad \text{whenever} \quad n \equiv b \mod q.$$

The symbol χ will always denote a character of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^*$ which we assume to be extended to $\mathbb{Z}$ by first identifying $(\mathbb{Z}/q\mathbb{Z})^*$ with the set

$$\{1 \leq n \leq q : (n, q) = 1\},$$

and defining

$$\chi(n) = \begin{cases} \chi(a) \text{ whenever } n \equiv a \mod q \text{ and } (a, q) = 1, \\ 0 \text{ if } (n, q) \neq 1. \end{cases}$$

Given any finite set of integers $\mathcal{A}$ we let $|\mathcal{A}|$ denote its cardinality.

1.5 Acknowledgement

The author would like to thank their family and in particular their parents and brother for continued support and patience despite extremely challenging circumstances.

The author would like to thank Igor Shparlinski for his guidance and support throughout the past four years, for being a role model as a person and a mathematician, for his patience with me as a student and for his ability to suggest papers and problems relevant to whatever I was working on.

The author would like to thank the School of Mathematics and Statistics at UNSW and in particular David Warton for his support throughout the course of his PhD.

The author would like to thank the Department of Computing and Macquarie University where he spent the first half of his PhD.

The author would like to than an anonymous referee for their suggestions and corrections of errors in Chapter 3.

The author would like to thank Roger Baker for his numerous suggestions concerning the presentation of arguments in Chapter 4.

Chapter 2

Rational Exponential Sums over the Divisor Function

2.1 Introduction

We consider a problem posed by Shparlinski [64, Problem 3.27] of bounding rational exponential sums over the divisor function. More specifically, for integers a and m with $(a, m) = 1$ and m odd we consider the sums

$$T_{a,m}(N) = \sum_{n=1}^{N} e_m(a\tau(n)), \tag{2.1}$$

where $e_m(z) = e^{2\pi iz/m}$ and $\tau(n)$ counts the number of divisors of n.

Arithmetic properties of the divisor function have been considered in a number of works, see for example [21, 24, 36, 47]. We are concerned mainly with congruence properties of the divisor function, which have been considered in [19, 51, 58]. Exponential sums over some other arithmetic functions have been considered in [2, 3].

Our first step in bounding the sums (2.1) uses a combinatorial decomposition of the integers based on Sathe [58]. This requires a sharper version of a result of Sathe [58, Lemma 1] concerning the distribution of the function $\omega(n)$ in residue classes, where $\omega(n)$ counts the number of distinct prime factors of n.

The ideas outlined above allow us to reduce the problem of bounding (2.1) to bounding sums of the form

$$S_m(r) = \sum_{n=1}^{t} e_m(r2^n), \tag{2.2}$$

where t denotes the order of $2 \pmod m$ and we may not necessarily have $(r, m) = 1$. Such sums have been well studied and we rely on previous work bounding these sums. See for example Bourgain [4], Heath-Brown and Konyagin [37] Korobov [45] and more recently Shkredov [62, 63].

2.1.1 Notation

If $p|n$ and θ has the property that p^θ is the largest power of p dividing n then we write $p^\theta||n$.

We let $\mathcal{S}$ denote the set of all square-free integers.

For integer $m \geq 3$ we let $\mathcal{M}_m$ the set of integers which are perfect m-th powers, $\mathcal{Q}_m$ the set of integers n, such that if $p^\theta||n$ then $2 \leq \theta \leq m-1$ and $\mathcal{K}$ the set of squarefull integers n defined by the property that if $p^\theta||n$ then $\theta \geq 2$.

Given an arbitrary set of integers $\mathcal{A}$, we let $\mathcal{A}(x)$ count the number of integers in $\mathcal{A}$ less than x. In particular we have

$$\mathcal{Q}_m(x) \leq \mathcal{K}(x) \ll x^{1/2}.$$

This implies that the sums

$$H(r, m) = \sum_{\substack{q \in \mathcal{Q}_m \\ \tau(q) \equiv r \pmod m}} \frac{h(q)}{q}, \qquad h(q) = \prod_{p|q} \left(1 + \frac{1}{p}\right)^{-1}, \tag{2.3}$$

converge.

We let $\zeta(s)$ denote the Riemann-zeta function,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \Re(s) > 1,$$

and $\Gamma(s)$ the Gamma function,

$$\Gamma(s) = \int_0^\infty x^{s-1} e^{-x} dx, \quad \Re(s) > 0.$$

For odd integer m we let t denote the order of $2 \pmod m$ and define

$$\alpha_t = 1 - \cos(2\pi/t). \tag{2.4}$$

2.2 Main Results

Theorem 2.1. *Suppose m is odd and sufficiently large. With notation as in (2.1), (2.2), (2.3) and (2.4) we have*

$$T_{a,m}(N) = \frac{\zeta(m)}{t}\frac{6}{\pi^2}\left(\sum_{r=0}^{m-1} H(r,m)S_m(ar)\right)N + O\left(tN(\log N)^{-\alpha_t}\right).$$

When $m = p$ is prime we use a different approach to save an extra power of $\log N$ in the asymptotic formula above, although our bound is worse in the t aspect.

Theorem 2.2. *Suppose $p > 2$ is prime, then*

$$T_{a,p}(N) = \frac{\zeta(p)}{t}\frac{6}{\pi^2}\left(\sum_{r=0}^{p-1} H(r,p)S_p(ar)\right)N + O\left(pN(\log N)^{-(\alpha_t+1)}\right).$$

Combining Theorem 2.1 with the main result from [4] we obtain a bound which is nontrivial for $N \geq e^{ct^{1/\alpha_t}}$ for some fixed constant c.

Theorem 2.3. *Suppose m is odd and sufficiently large, then for all $\varepsilon > 0$ there exists $\delta > 0$ such that if $t > m^{\varepsilon}$ then we have*

$$\max_{(a,m)=1} |T_{a,m}(N)| \ll \left(\frac{1}{m^{\delta}} + t(\log N)^{-\alpha_t}\right)N.$$

We may combine Theorem 2.2 with a number of different bounds for exponential sums over subgroups in prime fields to deduce corresponding bounds for exponential sums with the divisor function. The sharpness of such bounds usually depend on the order of the subgroup and in our setting this corresponds to the order of 2 mod p. For example, combining Theorem 2.2 with a bound of Shkredov [63] gives.

Theorem 2.4. *Suppose $p > 2$ is prime. If $t \leq p^{2/3}$ then we have*

$$\max_{(a,p)=1} |T_{a,p}(N)| \ll \left(t^{-1/2}p^{1/6}\log^{1/6} t + p\log N^{-(\alpha_t+1)}\right)N.$$

To deduce bounds for the quantity $\max_{(a,p)=1}|T_{a,p}(N)|$ which are sharper depending on the order of t relative to p one may consider combining Theorem 2.2 with results of Korobov [45] and Shkredov [62].

2.3 Combinatorial Decomposition

We use the decomposition of integers as in [58].

Lemma 2.5. *For any integer $m \geq 3$, any $n \in \mathbb{N}$ may be written uniquely in the form*

$$n = sqk,$$

with $s \in \mathcal{S}$, $q \in \mathcal{Q}_m$, $k \in \mathcal{M}_m$ and $\gcd(q, s) = 1$. For such a representation, we have

$$\tau(n) \equiv \tau(s)\tau(q) \pmod{m}.$$

Proof. We first fix an integer m. Given any integer n, let $n = p_1^{\alpha_1} \dots p_j^{\alpha_j}$ be the prime factorisation of n. We have

$$\tau(n) = (\alpha_1 + 1) \dots (\alpha_j + 1). \tag{2.5}$$

Let β_i be the remainder when α_i is divided by m. For some $k \in \mathcal{M}_m$ we have

$$n = kp_1^{\beta_1} \dots b_j^{\beta_j} = k \prod_{\beta_i = 1} p_i^{\beta_i} \prod_{\beta_i \neq 1} p_i^{\beta_i} = ksq,$$

with $s \in \mathcal{S}$, $q \in \mathcal{Q}_m$ and $\gcd(q, s) = 1$. Finally, we have from (2.5)

$$\tau(n) \equiv (\beta_1 + 1) \dots (\beta_j + 1) \equiv \tau(qs) \equiv \tau(q)\tau(s) \pmod{m},$$

since $\gcd(q, s) = 1$. □

2.4 Approximation of Preliminary Sums

Given an integer k, we let $\omega(k)$ denote the number of distinct prime factors of k. For a squarefree number q we let $A_q(X)$ count the number of non-negative integers $n \leq X$ such that any prime dividing n also divides q.

Techniques related to bounding $A_q(X)$ have been well studied in a number of different contexts. For example, Lehmer [46] interprets the problem geometrically as counting lattice points inside a tetrahedron. In the same paper Lehmer also considers an argument based on an idea of Rankin [57]. Hooley [41, Section 16] considers a related problem in which terms of $A_q(X)$ are weighted with certain multiplicative coefficients and uses the same idea of Rankin [57]. Granville [32] considers the problem of counting lattice points inside a tetrahedron from which bounds for $A_q(X)$ occur as a special case.

The problem of bounding $A_q(X)$ is also related to counting numbers with small prime factors to which we refer the reader to [23, 40, 50].

Lemma 2.6. *Suppose q is squarefree and let $A_q(X)$ be as above. We have*

$$A_q(X) \ll \frac{1}{\omega(q)!} \left(\log X + \omega(q)\right)^{\omega(q)}.$$

Proof. Suppose first that q is odd. Let $p_1, \dots, p_k$ be the distinct primes dividing q. We see that $A_q(X)$ counts the number of non-negative integers $h_1, \dots, h_k$ such that

$$h_1 \log p_1 + \cdots + h_k \log p_k \leq \log X. \tag{2.6}$$

The assumption q is odd implies that each $\log p_i \geq 1$. Hence if $h_1, \dots, h_k$ satisfy (2.6) then

$$h_1 + \cdots + h_k \leq \log X.$$

Since each h_i is integral, we see that

$$h_1 + \cdots + h_k \leq \lfloor \log X \rfloor. \tag{2.7}$$

The number of solutions to (2.7) is known to be (see for example [46, Equation 4])

$$\binom{k + \lfloor \log X \rfloor}{k}.$$

Writing $H = \lfloor \log X \rfloor$, this gives

$$A_q(X) \leq \frac{(k+H)!}{k!H!} \leq \frac{(H+k)^k}{k!} \leq \frac{(\log X + \omega(q))^{\omega(q)}}{\omega(q)!}. \tag{2.8}$$

Consider next when q is even. Letting $r = q/2$ we have

$$A_q(X) \leq \sum_{0 \leq h \leq \log X / \log 2} A_r(X 2^{-h}) \leq A_r(X) + \int_0^{\log X / \log 2} A_r(X 2^{-\alpha}) d\alpha.$$

An application of (2.8) gives

$$A_q(X) \leq \frac{(\log X + \omega(r))^{\omega(r)}}{\omega(r)!} + \frac{1}{\omega(r)!} \int_0^{\log X / \log 2} (\log X - \alpha \log 2 + \omega(r))^{\omega(r)} d\alpha,$$

which implies that

$$A_q(X) \ll \frac{1}{\omega(q)!} \left(\log X + \omega(q)\right)^{\omega(q)},$$

since $\omega(q) = \omega(r) + 1$. □

We use the following result of Selberg [61]. For related and more precise results see [65, II.6].

Lemma 2.7. *For any $z \in \mathbb{C}$*

$$\sum_{\substack{n\leq x\\ n\in\mathcal{S}}} z^{\omega(n)} = G(z)x(\log x)^{z-1} + O\left(x(\log x)^{\Re(z)-2}\right),$$

with

$$G(z) = \frac{1}{\Gamma(z)}\prod_p \left(1+\frac{z}{p}\right)\left(1-\frac{1}{p}\right)^z,$$

and the implied constant is uniform for all $|z| = 1$.

We combine Lemma 2.6 and Lemma 2.7 to give a sharper version of [58, Lemma 1].

Lemma 2.8. *For integers q, r and t let*

$$M(x,q,r,t) = \#\{\ n \leq x\ :\ n\in\mathcal{S},\quad \omega(n)\equiv r \pmod t,\quad (n,q)=1\}.$$

Then for $x \geq q$ we have

$$M(x,q,r,t) = \frac{6h(q)}{\pi^2 t}x + O\left(x^{1/2}(2\log x)^{\omega(q)} + x(\log x)^{-\alpha_t}\log\log q\right).$$

Proof. Suppose first q is squarefree. Let

$$S(a,x) = \sum_{\substack{n\leq x\\ n\in\mathcal{S}}} e_t(a\omega(n)),$$

and

$$S_1(a,q,x) = \sum_{\substack{n\leq x\\ n\in\mathcal{S}\\ (n,q)=1}} e_t(a\omega(n)).$$

Since the numbers $e_t(a\omega(n))$ with $(n,q)=1$ and $n\in\mathcal{S}$ are the coefficients of the Dirichlet series

$$\prod_{p\nmid q}\left(1+\frac{e_t(a)}{p^s}\right) = \prod_{p|q}\frac{1}{\left(1+\frac{e_t(a)}{p^s}\right)}\prod_p\left(1+\frac{e_t(a)}{p^s}\right),$$

we let the numbers a_n and b_n be defined by

$$\prod_{p|q}\frac{1}{\left(1+\frac{e_t(a)}{p^s}\right)} = \sum_{n=1}^{\infty}\frac{a_n}{n^s},$$
$$\prod_p\left(1+\frac{e_t(a)}{p^s}\right) = \sum_{n=1}^{\infty}\frac{b_n}{n^s}.$$

This gives

$$S(a,x) = \sum_{n\leq x} b_n,$$

and

$$S_1(a,q,x) = \sum_{n\leq x}\sum_{d_1d_2=n} b_{d_1}a_{d_2} = \sum_{n\leq x} a_n S(a,x/n).$$

Consider when $a \neq 0$. With notation as in Lemma 2.7

$$\begin{aligned}\sum_{n\leq x} a_n S(a,x/n) &= G(e_t(a))x\sum_{n\leq x}\frac{a_n}{n}(\log(x/n))^{e_t(a)-1} \\ &\quad + O\left(\sum_{n\leq x}|a_n|\frac{x}{n}(\log x/n)^{\cos(2\pi/t)-2}\right) \\ &\ll x(\log x)^{-(1-\cos(2\pi/t))}\sum_{n\leq x}\frac{|a_n|}{n} \\ &\ll x(\log x)^{-\alpha_t}\prod_{p|q}\left(1-\frac{1}{p}\right)^{-1}.\end{aligned}$$

Letting ϕ denote Euler's totient function, since

$$\prod_{p|q}\left(1-\frac{1}{p}\right)^{-1} = \frac{q}{\phi(q)} \ll \log\log q,$$

we see that

$$S_1(a,q,x) \ll x(\log x)^{-\alpha_t}\log\log q. \tag{2.9}$$

For $a = 0$, by [33, Theorem 334]

$$\begin{aligned}S_1(0,q,x) &= \sum_{n\leq x} a_n S(0,x/n) \\ &= \frac{6x}{\pi^2}\sum_{n\leq x}\frac{a_n}{n} + O\left(x^{1/2}\sum_{n\leq x}\frac{|a_n|}{n^{1/2}}\right) \\ &= \frac{6x}{\pi^2}\prod_{p|q}\left(1+\frac{1}{p}\right)^{-1} + O\left(x\sum_{n\geq x}\frac{|a_n|}{n} + x^{1/2}\sum_{n\leq x}\frac{|a_n|}{n^{1/2}}\right).\end{aligned}$$

Considering the first error term, with notation as in Lemma 2.6, we have

$$\sum_{n\leq t}|a_n| = A_q(t),$$

so that

$$\sum_{n\geq x}\frac{|a_n|}{n} \ll \int_x^\infty \frac{A_q(t)}{t^2}dt$$
$$\ll \frac{1}{\omega(q)!}\int_x^\infty \frac{(\log t+\omega(q))^{\omega(q)}}{t^2}dt. \tag{2.10}$$

From an application of the binomial theorem we get

$$\int_x^\infty \frac{(\log t+\omega(q))^{\omega(q)}}{t^2}dt = \sum_{n=0}^{\omega(q)}\binom{\omega(q)}{n}\omega(q)^{\omega(q)-n}\int_x^\infty \frac{(\log t)^n}{t^2}dt. \tag{2.11}$$

The integral

$$\int_x^\infty \frac{(\log t)^n}{t^2}dt,$$

is the n-th derivative of the function

$$H(z) = \int_x^\infty t^{z-2}dz = \frac{x^{z-1}}{1-z},$$

evaluated at $z=0$. By Cauchy's Theorem letting $\gamma\subset\mathbb{C}$ be the circle centred at 0 with radius $1/\log x$ we have

$$\int_x^\infty \frac{(\log t)^n}{t^2}dt = \frac{n!}{2\pi i}\int_\gamma \frac{x^{z-1}}{1-z}\frac{1}{z^{n+1}}dz \ll \frac{n!(\log x)^n}{x}.$$

Combining the above with (2.10) and (2.11) gives

$$\sum_{n\geq x}\frac{|a_n|}{n} \ll \frac{1}{x}\frac{\omega(q)^{\omega(q)}}{\omega(q)!}\sum_{n=0}^{\omega(q)}\binom{\omega(q)}{n}n!\left(\frac{\log x}{\omega(q)}\right)^n.$$

By Stirling's formula [49, Equation B.26]

$$\sum_{n=0}^{\omega(q)}\binom{\omega(q)}{n}n!\left(\frac{\log x}{\omega(q)}\right)^n \ll \sum_{n=0}^{\omega(q)}\binom{\omega(q)}{n}n^{1/2}\left(\frac{n}{e}\right)^n\left(\frac{\log x}{\omega(q)}\right)^n$$
$$\leq \omega(q)^{1/2}\sum_{n=0}^{\omega(q)}\binom{\omega(q)}{n}\left(\frac{\log x}{e}\right)^n$$
$$\ll \omega(q)^{1/2}\left(\frac{\log x}{e}+1\right)^{\omega(q)},$$

which implies that

$$\sum_{n\geq x}\frac{|a_n|}{n} \ll \frac{1}{x}\frac{\omega(q)^{\omega(q)+1/2}}{\omega(q)!}\left(\frac{\log x}{e}+1\right)^{\omega(q)}.$$

By the above and another application of Stirling's formula we arrive at

$$\sum_{n\geq x}\frac{|a_n|}{n}\ll\frac{1}{x}\left(\log x+e\right)^{\omega(q)}.$$

This gives

$$S_1(0,q,x)=\frac{6h(q)}{\pi^2}x+O\left(\left(\log x+e\right)^{\omega(q)}+x^{1/2}\sum_{n\leq x}\frac{|a_n|}{n^{1/2}}\right).$$

For the last term

$$\begin{aligned}\sum_{n\leq x}\frac{|a_n|}{n^{1/2}}&\leq\prod_{p|q}(1-p^{-1/2})^{-1}\\&=\prod_{p|q}(1+p^{-1/2})\prod_{p|q}\left(1-p^{-1}\right)^{-1}\ll 2^{\omega(q)}\log\log q,\end{aligned}$$

so that

$$S_1(0,q,x)=\frac{6h(q)}{\pi^2}x+O\left((2\log x)^{\omega(q)}+x^{1/2}2^{\omega(q)}\log\log q\right). \tag{2.12}$$

Since

$$\begin{aligned}M(x,q,r,t)&=\frac{1}{t}\sum_{a=0}^{t-1}e_t(-ar)S_1(a,q,x)\\&=\frac{1}{t}S_1(0,q,x)+\frac{1}{t}\sum_{a=1}^{t-1}e_t(-ar)S_1(a,q,x),\end{aligned}$$

we have from (2.9) and (2.12)

$$\begin{aligned}M(x,q,r,t)&=\frac{6h(q)}{\pi^2t}x\\&\quad+O\left((2\log x)^{\omega(q)}+x^{1/2}2^{\omega(q)}\log\log q+x(\log x)^{-\alpha_t}\log\log q\right).\end{aligned}$$

If q is not squarefree, repeating the above argument with q replaced by its squarefree part gives the desired result since the error term is increasing with q. □

2.5 Dirichlet Series Involving the Divisor Function

For complex s we write $s=\sigma+it$ with both σ and t real.

Lemma 2.9. *Let m be odd, χ a multiplicative character* mod m *and define*

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

For $\sigma>1$ we have

$$L(s,\chi,\tau)=\zeta(s)^{\chi(2)}F(s,\chi),$$

where $F(1,\chi)\neq 0$ and

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

for some coefficients $b(\chi,n)$. Uniformly over all χ we have

$$\sum_{n=1}^{\infty}\frac{|b(\chi,n)|}{n^{1/2+\delta}}=O(1),$$

for any $\delta>0$, with the implied constant depending only on δ.

Proof. Since both χ and τ are multiplicative, we have for $\sigma>1$

$$\begin{aligned}L(s,\chi,\tau)&=\prod_p\left(1+\sum_{n=1}^{\infty}\frac{\chi(\tau(p^n))}{p^{ns}}\right)\\&=\zeta(s)^{\chi(2)}F(s,\chi),\end{aligned}$$

with

$$F(s,\chi)=\prod_p\left(1+\sum_{n=1}^{\infty}\frac{\chi(n+1)}{p^{ns}}\right)\left(1-\frac{1}{p^s}\right)^{\chi(2)}.$$

We have

$$\begin{aligned}F(s,\chi)&=\prod_p\left(1-\frac{\chi(2)}{p^s}\right)\left(1+\frac{\chi(2)}{p^s}+\sum_{n=2}^{\infty}\frac{\chi(n+1)}{p^{ns}}\right)\times\\&\qquad\qquad\prod_p\left(1-\frac{\chi(2)}{p^s}\right)^{-1}\left(1-\frac{1}{p^s}\right)^{\chi(2)}\\&=F_1(s,\chi)F_2(s,\chi),\end{aligned}$$

where

$$\begin{aligned}F_1(s,\chi)&=\prod_p\left(1-\frac{\chi(2)}{p^s}\right)\left(1+\frac{\chi(2)}{p^s}+\sum_{n=2}^{\infty}\frac{\chi(n+1)}{p^{ns}}\right)\\&=\prod_p\left(1+\sum_{n=2}^{\infty}\frac{\chi(n+1)-\chi(2n)}{p^{ns}}\right),\end{aligned}\tag{2.13}$$

and

$$F_2(s,\chi) = \prod_p \left(1 - \frac{\chi(2)}{p^s}\right)^{-1} \left(1 - \frac{1}{p^s}\right)^{\chi(2)}.$$

Considering $F_2(s,\chi)$, we have for $\sigma > 1$

$$\begin{aligned} \log F_2(s,\chi) &= \sum_p \sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{\chi(2^n)}{p^{ns}} - \frac{\chi(2)}{p^{ns}} \right) \\ &= \sum_p \sum_{n=2}^{\infty} \frac{\chi(2^n) - \chi(2)}{n} \frac{1}{p^{ns}}. \end{aligned} \tag{2.14}$$

Since the sum in (2.14) converges absolutely for $s = 1$ we see that $F_2(1,\chi) \neq 0$.

To show that $F_1(1,\chi) \neq 0$, we note that the product in (2.13) converges absolutely for $s = 1$, hence it suffices to show that for each prime p we have

$$1 + \sum_{n=2}^{\infty} \frac{\chi(n+1) - \chi(2n)}{p^n} \neq 0.$$

Consider first when $p \geq 3$, then

$$\begin{aligned} 1 + \sum_{n=2}^{\infty} \frac{\chi(n+1) - \chi(2n)}{p^n} &\geq 1 - \frac{2}{p^2} \sum_{n=0}^{\infty} \frac{1}{p^n} = 1 - \frac{2}{p(p-1)} \\ &\geq \frac{2}{3}. \end{aligned}$$

For the case $p = 2$, we choose m satisfying $\chi(m+1) - \chi(2m) = 1$. Then we may write

$$\begin{aligned} 1 + \sum_{n=2}^{\infty} \frac{\chi(n+1) - \chi(2n)}{2^n} &= 1 + \sum_{\substack{n=2 \\ n \neq m}}^{\infty} \frac{\chi(n+1) - \chi(2n)}{2^n} + \frac{1}{2^m} \\ &\geq 1 - \sum_{n=1}^{\infty} \frac{1}{2^n} + \frac{1}{2^m} = \frac{1}{2^m}, \end{aligned}$$

which completes the proof that

$$F(1,\chi) \neq 0.$$

To prove the last part of the statement, since $|\chi(j) - \chi(k)| \leq 2$ for all integers k, j we see that the coefficients $b(\chi, n)$ in

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

satisfy

$$|b(\chi, n)| \leq c_n,$$

where the numbers c_n are defined by

$$\prod_p \left(1 + \sum_{j=2}^{\infty} \frac{2}{p^{js}}\right) \exp\left(\sum_p \sum_{j=2}^{\infty} \frac{2}{j} \frac{1}{p^{js}}\right) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}.$$

The function defined by the above formula converges uniformly in any halfplane $\sigma \geq \sigma_0 > 1/2$, so that

$$\sum_{n \leq X} c_n = O(X^{1/2+\varepsilon}),$$

and the last statement of the Lemma follows by partial summation. □

The following is [49, Theorem 7.18].

Lemma 2.10. *Suppose for each complex z we have a sequence $(b_z(n))_{n=1}^{\infty}$ such that the sum*

$$\sum_{n=1}^{\infty} \frac{|b_z(n)|(\log n)^{2R+1}}{n},$$

is uniformly bounded for $|z| \leq R$ and for $\sigma \geq 1$ let

$$F(s, z) = \sum_{n=1}^{\infty} \frac{b_z(m)}{m^s}.$$

Suppose for $\sigma > 1$ we have

$$\zeta(s)^z F(s, z) = \sum_{n=1}^{\infty} \frac{a_z(n)}{n^s},$$

for some $a_z(n)$ and let $S_z(x) = \sum_{n \leq x} a_z(n)$. Then for $x \geq 2$, uniformly over all $|z| \leq R$ we have

$$S_z(x) = \frac{F(1, z)}{\Gamma(z)} x(\log x)^{z-1} + O(x(\log x)^{\Re(z)-2}).$$

Combining Lemma 2.9 and Lemma 2.10 gives

Lemma 2.11. *For integer m let χ be a multiplicative character* $\bmod m$ *and let*

$$G(\chi) = \frac{1}{\Gamma(\chi(2))} \prod_p \left(\sum_{n=0}^{\infty} \frac{\chi(n+1)}{p^n}\right) \left(1 - \frac{1}{p}\right)^{\chi(2)}.$$

Then uniformly over all characters χ we have

$$\sum_{n \leq x} \chi(\tau(n)) = G(\chi) x(\log x)^{\chi(2)-1} + O\left(x(\log x)^{\Re(\chi(2))-2}\right). \tag{2.15}$$

We require a sharper estimate for the case of the principal character χ_0 to prime modulus.

Lemma 2.12. *Let p be an odd prime and χ_0 be the principal multiplicative character* mod p. *Then for some constant β_p and any $A > 0$ we have*

$$\sum_{n \leq x} \chi_0(\tau(n)) = \beta_p x + O\left(\frac{x}{\log^A x}\right).$$

Proof. We first note that since p is odd we have

$$\chi_0(2) = 1.$$

With notation as in Lemma 2.9, considering the Dirichlet series

$$L(s, \chi_0, \tau) = \sum_{n=1}^{\infty} \frac{\chi_0(\tau(n))}{n^s}.$$

We have

$$L(s, \chi_0, \tau) = \zeta(s) F(s, \chi_0), \tag{2.16}$$

where

$$\begin{aligned} F(s, \chi_0) &= \prod_{\substack{q \\ q \text{ prime}}} \left(1 + \sum_{n=1}^{\infty} \frac{\chi_0(n+1)}{q^{ns}}\right)\left(1 - \frac{1}{q^s}\right) \\ &= \prod_{\substack{q \\ q \text{ prime}}} \left(1 + \sum_{n=2}^{\infty} \frac{\chi_0(n+1) - \chi_0(n)}{q^{ns}}\right). \end{aligned}$$

Since $F(x, \chi_0)$ is analytic and bounded in any halfplane $\sigma > 1/2 + \varepsilon$ uniformly over all odd primes p, the stated bound follows by combining (2.16) with the Perron summation formulae and standard estimates for $\zeta(s)$. □

Lemma 2.13. *For any integer m we have*

$$\sum_{\substack{q \in \mathcal{K} \\ \tau(q) \equiv 0 \mod m}} \frac{1}{q} \ll \frac{1}{m^{\log 2/2}},$$

and if p is prime

$$\sum_{\substack{q \in \mathcal{K} \\ \tau(q) \equiv 0 \mod p}} \frac{1}{q} \ll \frac{1}{2^{p/2}}.$$

Proof. Suppose $\tau(q) \equiv 0 \pmod m$ and let $q = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be the prime factorization of q. We have

$$\tau(q) = (\alpha_1 + 1) \dots (\alpha_k + 1) \geq m.$$

By the arithmetic-geometric mean inequality

$$q \geq 2^{(\alpha_1+1)+\dots+(\alpha_k+1)-k} \geq 2^{k(\tau(q)^{1/k}-1)} \geq 2^{k(m^{1/k}-1)} \geq 2^{\log m} = m^{\log 2},$$

and since $\mathcal{K}(x) \ll x^{1/2}$ we get

$$\sum_{\substack{q \in \mathcal{K} \\ \tau(q) \equiv 0 \pmod m}} \frac{1}{q} \leq \sum_{\substack{q \in \mathcal{K} \\ q \geq m^{\log 2}}} \frac{1}{q} \ll \int_{m^{\log 2}}^{\infty} \frac{\mathcal{K}(x)}{x^2} dx \ll \frac{1}{m^{\log 2/2}}.$$

Suppose p is prime. If $\tau(n) \equiv 0 \pmod p$ then $n \geq 2^{p-1}$. Arguing as before we get

$$\sum_{\substack{q \in \mathcal{K} \\ \tau(q) \equiv 0 \pmod p}} \frac{1}{q} \ll \frac{1}{2^{p/2}}.$$

□

2.6 Proof of Theorem 2.1

By Lemma 2.5 we have

$$\begin{aligned}
\sum_{n=1}^{N} e_m(a\tau(n)) &= \sum_{\substack{k \in \mathcal{M}_m \\ k \leq N}} \sum_{\substack{q \in \mathcal{Q}_m \\ q \leq N/k}} \sum_{\substack{s \in \mathcal{S} \\ \gcd(s,q)=1 \\ s \leq N/qk}} e_m(a\tau(kqs)) \\
&= \sum_{\substack{k \in \mathcal{M}_m \\ k \leq N}} \sum_{\substack{q \in \mathcal{Q}_m \\ q \leq N/k}} \sum_{\substack{s \in \mathcal{S} \\ \gcd(s,q)=1 \\ s \leq N/qk}} e_m(a\tau(q)\tau(s)) \\
&= \sum_{\substack{k \in \mathcal{M}_m \\ k \leq N}} \sum_{\substack{q \in \mathcal{Q}_m \\ q \leq N/k}} \sum_{\substack{s \in \mathcal{S} \\ \gcd(s,q)=1 \\ s \leq N/qk}} e_m(a\tau(q)2^{\omega(s)}).
\end{aligned}$$

Taking $K = N^{1/2}$, partitioning summation over q depending on K and grouping together values of $2^{\omega(s)}$ in the same residue class $\bmod m$ gives

$$\sum_{n=1}^{N} e_m(a\tau(n)) = \sum_{\substack{k\in\mathcal{M}_m\\ k\le N}} \sum_{\substack{q\in\mathcal{Q}_m\\ q\le K/k}} \sum_{r=1}^{t} M(N/qk,q,r,t)e_m(a\tau(q)2^r) + \sum_{\substack{k\in\mathcal{M}_m\\ k\le N}} \sum_{\substack{q\in\mathcal{Q}_m\\ K/k<q\le N/k}} \sum_{r=1}^{t} M(N/qk,q,r,t)e_m(a\tau(q)2^r),$$

where $M(x,q,r,t)$ is defined as in Lemma 2.8. By choice of K we see that $N/qk \ge q$ when $q \le K/k$. Hence we may apply Lemma 2.8 to the first sum above

$$\sum_{n=1}^{N} e_m(a\tau(n)) = \frac{6}{\pi^2}\frac{N}{t} \sum_{\substack{k\in\mathcal{M}_m\\ k\le N}} \sum_{\substack{q\in\mathcal{Q}_m\\ q\le N/k}} \sum_{r=1}^{t} \frac{h(q)}{qk} e_m(a\tau(q)2^r)$$
$$+ O\left(\sum_{\substack{k\in\mathcal{M}_m\\ k\le N}} \sum_{\substack{q\in\mathcal{Q}_m\\ K/k<q\le N/k}} \frac{tN}{qk} + \sum_{\substack{k\in\mathcal{M}_m\\ k\le N}} \sum_{\substack{q\in\mathcal{Q}_m\\ q\le K/k}} \frac{Nt\log\log q}{qk} (\log(N/qk))^{-\alpha_t} \right)$$
$$+ O\left(\sum_{\substack{k\in\mathcal{M}_m\\ k\le N}} \sum_{\substack{q\in\mathcal{Q}_m\\ q\le K/k}} (2\log(N/kq))^{\omega(q)} \left(\frac{N}{kq}\right)^{1/2} \right).$$

Considering the first error term

$$\sum_{\substack{k\in\mathcal{M}_m\\ k\le N}} \sum_{\substack{q\in\mathcal{Q}_m\\ K/k<q\le N/k}} \frac{tN}{qk} \ll tN \int_K^N \frac{\mathcal{K}(x)}{x^2} dx \ll \frac{tN}{K^{1/2}}. \tag{2.17}$$

For the second error term, since the sum

$$\sum_{\substack{k\in\mathcal{M}_m\\ k\le N}} \sum_{\substack{q\in\mathcal{Q}_m\\ q\le K/k}} \frac{\log\log q}{qk},$$

is bounded uniformly in m as $K, N \to \infty$, we get

$$\sum_{\substack{k\in\mathcal{M}_m\\ k\le N}} \sum_{\substack{q\in\mathcal{Q}_m\\ q\le K/k}} \frac{Nt\log q}{qk} (\log(N/qk))^{-\alpha_t} \ll Nt\log(N/K)^{-\alpha_t} \sum_{\substack{k\in\mathcal{M}_m\\ k\le N}} \sum_{\substack{q\in\mathcal{Q}_m\\ q\le K/k}} \frac{\log\log q}{qk}$$
$$\ll Nt(\log(N/K))^{-\alpha_t}. \tag{2.18}$$

For the last term

$$\sum_{\substack{k\in\mathcal{M}_m\\k\le N}}\sum_{\substack{q\in\mathcal{Q}_m\\q\le K/k}}(e^4\log(N/kq))^{\omega(q)}\left(\frac{N}{kq}\right)^{1/2}\le N^{2/3}\sum_{\substack{n\in\mathcal{K}\\n\le N}}\left(\frac{1}{n}\right)^{2/3}(2\log N)^{\omega(n)}.$$

Since

$$\omega(n)\le(1+o(1))\frac{\log n}{\log\log n},$$

we get

$$\begin{aligned}
&N^{2/3}\sum_{\substack{k\in\mathcal{M}_m\\k\le N}}\sum_{\substack{q\in\mathcal{Q}_m\\q\le K/k}}(2\log N)^{\omega(q)}\left(\frac{1}{kq}\right)^{2/3}\\
&\qquad\le N^{2/3}(\log N)^{(1+o(1))\frac{\log N}{6\log\log N}}\sum_{\substack{n\in\mathcal{K}\\n\le N}}\left(\frac{1}{n}\right)^{2/3}(2(\log N)^{5/6})^{\omega(n)}\\
&\qquad\le N^{5/6+o(1)}\sum_{\substack{n\in\mathcal{K}\\n\le N}}\left(\frac{1}{n}\right)^{2/3}(2(\log N)^{5/6})^{\omega(n)}.
\end{aligned}$$

We may bound the last sum on the right by noting

$$\sum_{\substack{n\in\mathcal{K}\\n\le N}}\left(\frac{1}{n}\right)^{2/3}(2(\log N)^{5/6})^{\omega(n)}\le\prod_p\left(1+2(\log N)^{5/6}\sum_{k=2}^{\infty}\frac{1}{p^{2k/3}}\right).$$

Taking logarithms we see that

$$\begin{aligned}
\log\left(\prod_p\left(1+2(\log N)^{5/6}\sum_{k=2}^{\infty}\frac{1}{p^{2k/3}}\right)\right)&=\sum_p\log\left(\left(1+\frac{2(\log N)^{5/6}}{p^{4/3}}\frac{p^{2/3}}{p^{2/3}-1}\right)\right)\\
&\le 2(\log N)^{5/6}\sum_p\frac{1}{p^{4/3}}\frac{p^{2/3}}{p^{2/3}-1}\\
&\ll(\log N)^{5/6}.
\end{aligned}$$

This implies that for some absolute constant c

$$\sum_{\substack{k\in\mathcal{M}_m\\k\le N}}\sum_{\substack{q\in\mathcal{Q}_m\\q\le K/k}}(e^4\log(N/kq))^{\omega(q)}\left(\frac{N}{kq}\right)^{1/2}\ll N^{5/6+o(1)}e^{c(\log N)^{5/6}}.\tag{2.19}$$

Combining (2.17), (2.18) and (2.19) gives

$$\sum_{n=1}^{N} e_m(a\tau(n)) = \frac{6}{\pi^2}\frac{N}{t}\sum_{\substack{k\in\mathcal{M}_m\\ k\le N}}\frac{1}{k}\sum_{\substack{q\in\mathcal{Q}_m\\ q\le N/k}}\frac{h(q)}{q}\sum_{r=1}^{t} e_m(a\tau(q)2^r) + O\left(Nt(\log(N/K))^{-\alpha_t} + \frac{tN}{K^{1/2}} + N^{5/6+o(1)}e^{c(\log N)^{5/6}}\right),$$

and recalling the choice of K we get

$$\sum_{n=1}^{N} e_m(a\tau(n)) = \frac{6}{\pi^2}\frac{N}{t}\sum_{\substack{k\in\mathcal{M}_m\\ k\le N}}\frac{1}{k}\sum_{\substack{q\in\mathcal{Q}_m\\ q\le N/k}}\frac{h(q)}{q}\sum_{r=1}^{t} e_m(a\tau(q)2^r) + O\left(Nt(\log N)^{-\alpha_t}\right). \quad (2.20)$$

For the main term

$$\sum_{\substack{k\in\mathcal{M}_m\\ k\le N}}\frac{1}{k}\sum_{\substack{q\in\mathcal{Q}_m\\ q\le N/k}}\frac{h(q)}{q}\sum_{r=1}^{t} e_m(a\tau(q)2^r)$$
$$= \sum_{\substack{k\in\mathcal{M}_m\\ k\le N}}\frac{1}{k}\sum_{q\in\mathcal{Q}_m}\frac{h(q)}{q}\sum_{r=1}^{t} e_m(a\tau(q)2^r) + O\left(t\sum_{\substack{k\in\mathcal{M}_m\\ k\le N}}\frac{1}{k}\left(\frac{k}{N}\right)^{1/2}\right),$$

and hence

$$\sum_{\substack{k\in\mathcal{M}_m\\ k\le N}}\frac{1}{k}\sum_{\substack{q\in\mathcal{Q}_m\\ q\le N/k}}\frac{h(q)}{q}\sum_{r=1}^{t} e_m(a\tau(q)2^r) = \sum_{k\in\mathcal{M}_m}\frac{1}{k}\sum_{q\in\mathcal{Q}_m}\frac{h(q)}{q}\sum_{r=1}^{t} e_m(a\tau(q)2^r) + O\left(\frac{t}{N^{1/2}}\right)$$
$$= \zeta(m)\sum_{q\in\mathcal{Q}_m}\frac{h(q)}{q}\sum_{r=1}^{t} e_m(a\tau(q)2^r) + O\left(\frac{t}{N^{1/2}}\right).$$

This gives

$$\sum_{n=1}^{N} e_m(a\tau(n)) = \frac{\zeta(m)}{t}\frac{6}{\pi^2}\left(\sum_{r \pmod m} H(r,m)S_m(ar)\right)N + O\left(tN(\log N)^{-\alpha_t}\right).$$

2.7 Proof of Theorem 2.2

Let

$$C(p,r,N) = \#\{n \le N : \tau(n) \equiv r \pmod p\},$$

so that

$$\sum_{n=1}^{N} e_p(a\tau(n)) = \sum_{r=0}^{p-1} C(p,r,N)e_m(ar). \quad (2.21)$$

Suppose $(r,p)=1$, using orthogonality of characters, Lemma 2.11 and Lemma 2.12

$$\begin{aligned}
C(p,r,N) &= \frac{1}{p-1}\sum_{n=1}^{N}\sum_{\chi(\mathrm{mod}\ p)}\overline{\chi}(r)\chi(\tau(n)) \\
&= \frac{1}{p-1}\sum_{n=1}^{N}\chi_0(\tau(n)) + \frac{1}{p-1}\sum_{n=1}^{N}\sum_{\substack{\chi(\mathrm{mod}\ p)\\ \chi\neq\chi_0}}\overline{\chi}(r)\chi(\tau(n)) \\
&= \frac{\beta_p}{p-1}N + \frac{1}{p-1}\sum_{\chi(2)=1}\overline{\chi}(r)G(\chi)N + \frac{1}{p-1}\sum_{\chi(2)\neq 1}\overline{\chi}(r)G(\chi)N(\log N)^{\chi(2)-1} \\
&\quad + O\left(N(\log N)^{-(\alpha_p+1)}\right),
\end{aligned}$$

where β_p is defined as in Lemma 2.12. For $r=0$, we have by Lemma 2.12

$$C(p,0,N) = \sum_{n=1}^{N}(1-\chi_0(\tau(n))) = c_pN + O\left(N(\log N)^{-2}\right),$$

for some constant c_p. Hence from (2.21)

$$\begin{aligned}
\sum_{n=1}^{N}e_p(a\tau(n)) &= C_pN + O\left(pN(\log N)^{-(\alpha_t+1)}\right) \\
&\quad + \frac{N}{p-1}\sum_{r=1}^{p-1}\left(\sum_{\chi(2)=1}\overline{\chi}(r)G(\chi)e_p(ar) + \sum_{\chi(2)\neq 1}\overline{\chi}(r)e_p(ar)G(\chi)(\log N)^{\chi(2)-1}\right) \\
&= A_pN + \frac{N}{p-1}\sum_{\chi(2)\neq 1}G(\chi)(\log N)^{\chi(2)-1}\sum_{r=1}^{p-1}\overline{\chi}(r)e_p(ar) \\
&\quad + O\left(pN(\log N)^{-(\alpha_t+1)}\right),
\end{aligned}$$

for some constant A_p. If $\chi(2)\neq 1$ then we have

$$\left|\sum_{r=1}^{p-1}\overline{\chi}(r)e_p(ar)\right| = p^{1/2},$$

so that

$$\sum_{n=1}^{N}e_p(a\tau(n)) = A_pN + O\left(p^{1/2}N(\log N)^{-\alpha_t} + pN(\log N)^{-(\alpha_t+1)}\right).$$

Since we may assume $N > pN(\log N)^{-(\alpha_t+1)}$ as otherwise our bound is trivial, the above simplifies to

$$\sum_{n=1}^{N} e_p(a\tau(n)) = A_p N + O\left(pN(\log N)^{-(\alpha_t+1)}\right). \tag{2.22}$$

Finally, comparing (2.22) with the leading term in the asymptotic formula from Theorem 2.1, we see that

$$A_p = \frac{\zeta(p)}{t}\frac{6}{\pi^2}\left(\sum_{r=0}^{p-1} H(r,p)S_p(ar)\right).$$

2.8 Proof of Theorem 2.3

Considering the main term in Theorem 2.1

$$\begin{aligned}\left|\sum_{r=0}^{m-1} H(r,m)S_m(ar)\right| &\leq \sum_{d|m}\left|\sum_{\substack{r=0\\ \gcd(r,m)=d}}^{m-1} H(r,m)S_m(ar)\right| \\ &\leq \sum_{d|m}\left(\sum_{\substack{r=0\\ \gcd(r,m)=d}}^{m-1} H(r,m)\right)\max_{\gcd(\lambda,m)=d}|S_m(\lambda)|.\end{aligned}$$

Writing $c = \log 2/2$, by Lemma 2.13

$$\begin{aligned}\sum_{\substack{r=0\\ \gcd(r,m)=d}}^{m-1} H(r,m) &= \sum_{\substack{r=0\\ \gcd(r,m)=d}}^{m-1}\sum_{\substack{q\in\mathcal{Q}_m\\ \tau(q)\equiv r \pmod m}}\frac{h(q)}{q} \\ &\leq \sum_{\substack{q\in\mathcal{K}\\ \tau(q)\equiv 0 \pmod d}}\frac{1}{q} \ll \frac{1}{d^c},\end{aligned}$$

which gives

$$\sum_{r=0}^{m-1} H(r,m)S_m(ar) \ll \sum_{d|m}\frac{1}{d^c}\max_{\gcd(\lambda,m)=d}|S_m(\lambda)|. \tag{2.23}$$

Suppose $\gcd(\lambda,m) = d$, so that we may write

$$\lambda = d\lambda' \quad \text{and} \quad m = dm,'$$

for some λ' and m' with $\gcd(\lambda', m') = 1$. Let t_d denote the order of $2 \mod m'$, so that

$$S_m(\lambda) = \sum_{n=1}^{t} e_m(\lambda 2^n) = \frac{t}{t_d} \sum_{n=1}^{t_d} e_{m'}(\lambda' 2^n).$$

By the main result of [4], if $t_d \geq (m/d)^\varepsilon$ then for some $\delta > 0$ we have

$$S_m(\lambda) \ll \left(\frac{d}{m}\right)^\delta t. \tag{2.24}$$

Suppose $t \geq m^\varepsilon$, then since

$$t_d \geq \frac{t}{d} \geq \frac{m^{\varepsilon/2}}{d} m^{\varepsilon/2},$$

if $d \leq m^{\varepsilon/2}$ then we have $t_d \geq (m/d)^{\varepsilon/2}$. An application of (2.24) gives

$$S_m(\lambda) \ll \left(\frac{d}{m}\right)^\delta t \ll \frac{t}{m^{\delta_0}}.$$

Hence by (2.23) for some $\delta_1 > 0$

$$\begin{aligned}\sum_{r=0}^{m-1} H(r,m) S_m(ar) &\ll \sum_{\substack{d|m \\ d \leq m^{\varepsilon/2}}} \frac{1}{d^c} \max_{\gcd(\lambda,m)=d} |S_m(\lambda)| + \sum_{\substack{d|m \\ d \geq m^{\varepsilon/2}}} \frac{1}{d^c} \max_{\gcd(\lambda,m)=d} |S_m(\lambda)| \\ &\ll \sum_{\substack{d|m \\ d \leq m^{\varepsilon/2}}} \frac{t}{m^{\delta_1}} + \sum_{\substack{d|m \\ d \geq m^{\varepsilon/2}}} \frac{1}{m^{\delta_1}} = \frac{\tau(m)}{m^{\delta_1}} t, \end{aligned} \tag{2.25}$$

and the result follows combining (2.25) with Theorem 2.1.

2.9 Proof of Theorem 2.4

By Lemma 2.13

$$\begin{aligned}\sum_{r=0}^{p-1} H(r,p) S_p(ar,t) &= \sum_{r=1}^{p-1} H(r,p) S_p(ar) + tH(0,p) \\ &\ll \frac{t}{2^{p/2}} + \left(\sum_{r=1}^{p-1} H(r,p)\right) \max_{\gcd(\lambda,p)=1} |S_p(\lambda)| \\ &\ll \frac{t}{2^{p/2}} + \max_{\gcd(\lambda,p)=1} |S_p(\lambda)|,\end{aligned}$$

and by [63, Theorem 1]

$$\max_{\gcd(\lambda,p)=1} |S_p(\lambda)| \leq t^{1/2} p^{1/6} \log^{1/6} t,$$

from which the result follows.

Chapter 3

Character Sums over Shifted Primes

3.1 Introduction

Let q be an arbitrary positive integer and let χ be a primitive non-principal multiplicative character $\bmod q$. Our goal is to estimate character sums of the form

$$S_a(q;N) = \sum_{n \le N} \Lambda(n)\chi(n+a), \tag{3.1}$$

where a is an integer relatively prime to q and $\Lambda(n)$ is the Von Mangoldt function defined by

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

For prime modulus q, Karatsuba [43] has given a nontrivial estimate of the sums $S_a(q;N)$ in the range $N > q^{1/2+\varepsilon}$. Recently, much more general sums over primes have been considered by Fouvry, Kowalski and Michel [25]. A special case of their result (see [25, Corollary 1.12]) gives nontrivial bounds for character sums to prime modulus q with a very general class of rational functions over primes and is nontrivial provided $N > q^{3/4+\varepsilon}$. Rakhmonov [54, 55] has shown that nontrivial cancellations in the sums $S_a(q;N)$ also occur in the case of general modulus q, but only in the narrower range $N > q^{1+\varepsilon}$. This range has been extended by Friedlander, Gong and Shparlinski [26] to $N > q^{8/9+\varepsilon}$ where the bound

$$|S_a(q;N)| \le (N^{7/8}q^{1/9} + N^{33/32}q^{-1/18})q^{o(1)}, \tag{3.2}$$

is given for $N \le q^{16/9}$. Recently Rakhmonov [56] has shown that

$$S_a(q;N) \ll Ne^{-\sqrt{\log q}}, \tag{3.3}$$

provided $N \ge q^{5/6+o(1)}$. Comparing the bound of Rakhmonov (3.3) with the bound of Friedlander, Gong and Shparlinski (3.2), we see that (3.3) is valid for a wider range of the parameter N although is quantitatively much weaker than (3.2). In this paper we improve on the strength of Rakhmonov's bound.

3.2 Main Result

Our main result is as follows.

Theorem 3.1. *For $N \le q$ we have*

$$|S_a(q;N)| \le \left(Nq^{-1/24} + q^{5/42}N^{6/7}\right) q^{o(1)}.$$

We see that Theorem 3.1 is nontrivial provided $N \ge q^{5/6+o(1)}$ and can be considered as comparable on a quantitative level to the bound of Friedlander, Gong and Shparlinski (3.2) as it also gives a power saving.

3.3 Reduction to Bilinear Forms

As in [26] our basic tool is the Vaughan identity, see [60].

Lemma 3.2. *For any complex-valued function $f(n)$ and any real numbers U, $V > 1$ with $UV \le N$, we have*

$$\sum_{1\le n\le N} \Lambda(n)f(n) \ll \Sigma_1 + \Sigma_2 + \Sigma_3 + |\Sigma_4|,$$

where

$$\begin{aligned}
\Sigma_1 &= \left|\sum_{n\le U} \Lambda(n)f(n)\right|,\\
\Sigma_2 &= (\log UV)\sum_{v\le UV}\left|\sum_{s\le N/v} f(sv)\right|,\\
\Sigma_3 &= (\log N)\sum_{v\le V}\max_{w\ge 1}\left|\sum_{w\le s\le N/v} f(sv)\right|,\\
\Sigma_4 &= \sum_{\substack{k\ell\le N\\ k>V,\,\ell>U}} \Lambda(\ell)\sum_{d|k,\,d\le V}\mu(d)f(k\ell).
\end{aligned}$$

where $\mu(d)$ denotes the Möbius function and is defined by

$$\mu(d) = \begin{cases} (-1)^{\omega(d)}, & \text{if } d \text{ squarefree,} \\ 0, & \text{otherwise,} \end{cases}$$

and $\omega(d)$ counts the number of distinct prime factors of d.

3.4 The Pólya-Vinogradov Bound

The following is [26, Lemma 4].

Lemma 3.3. *For any integers d, M, N, a with $(a, q) = 1$ and any primitive character χ mod q we have*

$$\left| \sum_{M < n \le M+N} \chi(dn + a) \right| \le (d, q) \frac{N}{q^{1/2}} + q^{1/2+o(1)}.$$

In [26], Lemma 3.3 was used to show [26, Lemma 5] which we state as follows.

Lemma 3.4. *For any integers M, N, a with $(a, q) = 1$ and any primitive character χ mod q we have*

$$\left| \sum_{\substack{M < n \le M+N \\ (n,q)=1}} \chi(n + a) \right| \le q^{1/2+o(1)} + Nq^{-1/2}.$$

3.5 Burgess Bounds

The techniques of [26] combine a basic sieve with the amplification method to reduce bounding the sums

$$\sum_{\substack{n \le N \\ (n,q)=1}} \chi(n + a),$$

to bounding the mean values

$$\sum_{v_1,\dots,v_{2r}=1}^{V} \left| \sum_{x=1}^{q} \chi\left(\prod_{i=1}^{r} (x + dv_i) \right) \overline{\chi}\left(\prod_{i=r+1}^{2r} (x + dv_i) \right) \right|, \quad r = 2, 3. \tag{3.4}$$

The argument of [26] proceeds to bound the mean values (3.4) by completing outer summation to result in sums of the form

$$\sum_{v_1,\dots,v_{2r}=1}^{dV} \left| \sum_{x=1}^{q} \chi\left(\prod_{i=1}^{r} (x + v_i) \right) \overline{\chi}\left(\prod_{i=r+1}^{2r} (x + v_i) \right) \right| \quad r = 2, 3.$$

We give a slight improvement on [26] by modifying the method of Burgess [9, 13] to bound the mean values (3.4) directly.

3.5.1 The Case $r = 2$

We use a special case of [9, Lemma 7].

Lemma 3.5. *For integer q let χ be a primitive character* mod q *and let*

$$f_1(x) = (x - dv_1)(x - dv_2), \quad f_2(x) = (x - dv_3)(x - dv_4).$$

Suppose at least 3 *of the integers v_1, v_2, v_3 and v_4 are distinct and define*

$$A_i = \prod_{j \neq i} (dv_i - dv_j).$$

Then we have

$$\left| \sum_{x=1}^{q} \chi(f_1(x)) \overline{\chi}(f_2(x)) \right| \leq 8^{\omega(q)} q^{1/2} (q, A_i),$$

for some $A_i \neq 0$.

The next Lemma is based on Lemma 3.5 and ideas from the proof of [9, Lemma 8].

Lemma 3.6. *For any primitive character χ* mod q *and any positive integer V we have*

$$\sum_{v_1, \dots, v_4 = 1}^{V} \left| \sum_{x=1}^{q} \chi \left(\prod_{i=1}^{2} (x + dv_i) \right) \overline{\chi} \left(\prod_{i=3}^{4} (x + dv_i) \right) \right| \leq (V^2 q + (d, q)^3 q^{1/2} V^4) q^{o(1)}.$$

Proof. We divide the outer summation of

$$\sum_{v_1, v_2, v_3, v_4 = 1}^{V} \left| \sum_{x=1}^{q} \chi \left(\prod_{i=1}^{2} (x + dv_i) \right) \overline{\chi} \left(\prod_{i=3}^{4} (x + dv_i) \right) \right|,$$

into two sets. In the first set we put all v_1, v_2, v_3 and v_4 which contain at most 2 distinct numbers and we put the remaining v_1, v_2, v_3 and v_4 into the second set. The number of elements in the first set is $\ll V^2$ and for these sets we estimate the inner sum trivially. This gives

$$\sum_{v_1, \dots, v_4 = 1}^{V} \left| \sum_{x=1}^{q} \chi \left(\prod_{i=1}^{2} (x + dv_i) \right) \overline{\chi} \left(\prod_{i=3}^{4} (x + dv_i) \right) \right| \ll$$
$$qV^2 + \sum_{v_1, \dots, v_4 = 1}^{V}{}' \left| \sum_{x=1}^{q} \chi \left(\prod_{i=1}^{2} (x + dv_i) \right) \overline{\chi} \left(\prod_{i=3}^{4} (x + dv_i) \right) \right|,$$

where the last sum is restricted to v_1, v_2, v_3 and v_4 which contain at least 3 distinct numbers. With notation as in Lemma 3.5 we have

$$\sum_{v_1,\dots,v_4=1}^{V}{}' \left| \sum_{x=1}^{q} \chi\left(f_1(x)\right) \overline{\chi}\left(f_2(x)\right) \right| \leq q^{1/2+o(1)} \sum_{v_1,\dots,v_4=1}^{V}{}' \sum_{\substack{i=1 \\ A_i \neq 0}}^{4} (A_i, q).$$

Since

$$A_i = \prod_{i \neq j} (dv_i - dv_j) = d^3 \prod_{i \neq j} (v_i - v_j) = d^3 A_i',$$

we see that

$$\sum_{v_1,\dots,v_4=1}^{V}{}' \sum_{\substack{i=1 \\ A_i \neq 0}}^{4} (A_i, q) \leq (d^3, q) \sum_{v_1,\dots,v_4=1}^{V}{}' \sum_{\substack{i=1 \\ A_i \neq 0}}^{4} (A_i', q),$$

and in [9, Lemma 8] it is shown

$$\sum_{v_1,\dots,v_4=1}^{V}{}' \sum_{\substack{i=1 \\ A_i \neq 0}}^{4} (A_i', q) \leq V^4 q^{o(1)},$$

from which the result follows. □

Using Lemma 3.6 in the proof of [26, Lemma 10] we arrive at the following bound.

Lemma 3.7. *For any primitive character* $\chi \mod q$ *and integers* M, N, a *and* d *satisfying*

$$N \leq q^{5/8} d^{-5/4}, \quad d \leq q^{1/6}, \quad (a, q) = 1,$$

we have

$$\left| \sum_{M < n \leq M+N} \chi(dn + a) \right| \leq q^{3/16+o(1)} d^{3/8} N^{1/2}.$$

Proof. We proceed by induction on N. Since the result is trivial for $N \leq q^{3/8}$ this forms the basis of the induction. We define

$$U = [0.25 N d^{3/2} q^{-1/4}], \quad V = [0.25 d^{-3/2} q^{1/4}],$$

and let

$$\mathcal{U} = \{\ 1 \leq u \leq U\ :\ (u, dq) = 1\ \}, \quad \mathcal{V} = \{\ 1 \leq v \leq V\ :\ (v, q) = 1\ \}.$$

By the inductive assumption, for any $\varepsilon > 0$ and integer $h \le UV < N$ we have

$$\left|\sum_{M<n\le M+N}\chi(dn+a)\right| \le \left|\sum_{M<n\le M+N}\chi(d(n+h)+a)\right| + 2q^{3/16+\varepsilon}d^{3/8}h^{1/2},$$

for sufficiently large q. Hence

$$\left|\sum_{M<n\le M+N}\chi(dn+a)\right| \le \frac{1}{|\mathcal{U}||\mathcal{V}|}|W| + 2q^{3/16+\varepsilon}d^{3/8}(UV)^{1/2},$$

where

$$\begin{aligned} W &= \sum_{u\in\mathcal{U}}\sum_{v\in\mathcal{V}}\sum_{M<n\le M+N}\chi(d(n+uv)+a) \\ &= \sum_{u\in\mathcal{U}}\chi(u)\sum_{M<n\le M+N}\sum_{v\in\mathcal{V}}\chi((dn+a)u^{-1}+dv). \end{aligned}$$

We have

$$|W| \le \sum_{x=1}^{q}\nu(x)\left|\sum_{v\in\mathcal{V}}\chi(x+dv)\right|,$$

where $\nu(x)$ counts the number of representations $x \equiv (dn+a)u^{-1} \mod q$ with $M < n \le M+N$ and $u \in \mathcal{U}$.

Two applications of Hölder's inequality gives

$$|W|^4 \le \left(\sum_{x=1}^{q}\nu^2(x)\right)\left(\sum_{x=1}^{q}\nu(x)\right)^2\sum_{x=1}^{q}\left|\sum_{v\in\mathcal{V}}\chi(x+dv)\right|^4.$$

From the proof of [26, Lemma 7] we have

$$\sum_{x=1}^{q}\nu(x) = N\#\mathcal{U}, \quad \sum_{x=1}^{q}\nu^2(x) \le \left(\frac{dNU}{q}+1\right)NUq^{o(1)},$$

and by Lemma 3.6

$$\begin{aligned} \sum_{x=1}^{q}\left|\sum_{v\in\mathcal{V}}\chi(x+dv)\right|^4 &= \sum_{v_1,\dots v_4\in\mathcal{V}}\sum_{x=1}^{q}\chi\left(\prod_{i=1}^{2}(x+dv_i)\right)\overline{\chi}\left(\prod_{i=3}^{4}(x+dv_i)\right) \\ &\le \sum_{v_1,\dots v_4=1}^{V}\left|\sum_{x=1}^{q}\chi\left(\prod_{i=1}^{2}(x+dv_i)\right)\overline{\chi}\left(\prod_{i=3}^{4}(x+dv_i)\right)\right| \\ &\ll V^2q^{1+o(1)}, \end{aligned}$$

since $V \le d^{-3/2}q^{1/4}$.

Combining the above bounds we get

$$|W|^4 \leq \left(\frac{dNU}{q}+1\right) NU(N|\mathcal{U}|)^2V^2q^{1+o(1)}.$$

Since

$$|\mathcal{U}| = Uq^{o(1)}, \quad |\mathcal{V}| = Vq^{o(1)},$$

we have

$$\left|\sum_{M<n\leq M+N}\chi(dn+a)\right| \leq \left(\frac{d^{1/4}N}{V^{1/2}}+\frac{q^{1/4}N^{3/4}}{U^{1/4}V^{1/2}}\right)q^{o(1)}+2q^{3/16+\varepsilon}d^{3/8}(UV)^{1/2}.$$

Recalling the choice of U and V gives

$$\left|\sum_{M<n\leq M+N}\chi(dn+a)\right| \leq \left(\frac{dN}{q^{1/8}}+q^{3/16}d^{3/8}N^{1/2}\right)q^{o(1)}+\frac{1}{2}q^{3/16+\varepsilon}d^{3/8}N^{1/2}.$$

Since by assumption

$$N \leq q^{5/8}d^{-5/4},$$

we see that for sufficiently large q

$$\begin{aligned}\left|\sum_{M<n\leq M+N}\chi(dn+a)\right| &\leq q^{3/16}d^{3/8}N^{1/2}q^{o(1)}+\frac{1}{2}q^{3/16+\varepsilon}d^{3/8}N^{1/2}\\ &\leq q^{3/16+\varepsilon}d^{3/8}N^{1/2}.\end{aligned}$$

□

In [26, Lemma 11] it is shown that

$$\left|\sum_{\substack{M<n\leq M+N\\(n,q)=1}}\chi(n+a)\right| \leq q^{3/20+o(1)}N^{3/5},$$

provided $N \leq q^{5/8}$. Our next Lemma can be considered as an improvement on this bound.

Lemma 3.8. *Let χ be a primitive character* mod q *and suppose $(a,q)=1$. For $N \leq q^{43/72}$ we have*

$$\left|\sum_{\substack{M<n\leq M+N\\(n,q)=1}}\chi(n+a)\right| \leq q^{3/16+o(1)}N^{1/2}.$$

Proof. We have

$$\left|\sum_{\substack{M<n\le M+N\\(n,q)=1}}\chi(n+a)\right| = \left|\sum_{d|q}\mu(d)\sum_{M/d<n\le (M+N)/d}\chi(dn+a)\right|$$
$$\le \sum_{d|q}\left|\sum_{M/d<n\le (M+N)/d}\chi(dn+a)\right|.$$

Let

$$Z = \left\lfloor \frac{N^{1/2}}{q^{3/16}} \right\rfloor,$$

and partition outer summation according to Z. By Lemma 3.7 we have

$$\sum_{d|q}\left|\sum_{M/d<n\le (M+N)/d}\chi(dn+a)\right| =$$
$$\sum_{\substack{d|q\\d\le Z}}\left|\sum_{M/d<n\le (M+N)/d}\chi(dn+a)\right| + \sum_{\substack{d|q\\d>Z}}\left|\sum_{M/d<n\le (M+N)/d}\chi(dn+a)\right|$$
$$\le \sum_{\substack{d|q\\d\le Z}} q^{3/16+o(1)}d^{-1/8}N^{1/2} + \sum_{\substack{d|q\\d>Z}}\frac{N}{d}.$$

By choice of Z we get

$$\sum_{\substack{d|q\\d\le Z}} q^{3/16+o(1)}d^{-1/8}N^{1/2} + \sum_{\substack{d|q\\d>Z}}\frac{N}{d} \le \left(q^{3/16}N^{1/2} + \frac{N}{Z}\right)q^{o(1)} \le q^{3/16+o(1)}N^{1/2},$$

which gives the desired bound.

It remains to check that the conditions of Lemma 3.7 are satisfied. For each $d|q$ with $d \le Z$ we need

$$\frac{N}{d} \le q^{5/8}d^{-5/4}, \quad d \le q^{1/6},$$

which on recalling the choice of Z is satisfied for $N \le q^{43/72}$. □

3.5.2 The Case $r = 3$

Throughout this section we let

$$f_1(x) = (x+dv_1)(x+dv_2)(x+dv_3), \quad f_2(x) = (x+dv_4)(x+dv_5)(x+dv_6), \tag{3.5}$$

and

$$F(x) = f_1'(x)f_2(x) - f_1(x)f_2'(x), \tag{3.6}$$

and write $\mathbf{v} = (v_1, \dots v_6)$. We generalize the argument of Burgess [13] to give an upper bound for the cardinality of the set

$$\begin{aligned}\mathcal{A}(s, s') = \{\mathbf{v} \in \mathbb{Z}^6 \ : \ & 0 < v_i \le V, \text{ there exists an } x \text{ such that} \\ & (s, f_1(x)f_2(x)) = 1, \ s|F(x), \ s|F'(x), \ s'|F''(x)\},\end{aligned}$$

which will then be combined with the proof of [13, Theorem 2] to bound the sums (3.4). The proof of the following Lemma is the same as [13, Lemma 3].

Lemma 3.9. *Let $s'|s$ and consider the relations*

$$(\lambda, s) = 1, \quad (f_1(-t), s/s') = 1, \tag{3.7}$$

$$6(f_1(X) + \lambda f_2(X)) \equiv 6(1+\lambda)(X+t)^3 \mod s, \tag{3.8}$$

$$6(1+\lambda) \equiv 0 \mod s'. \tag{3.9}$$

Let

$$\begin{aligned}\mathcal{A}_1(s, s') = \{(\mathbf{v}, \ \lambda, \ t) \in \mathbb{Z}^8 \ : \ & 0 < v_i \le V, \ v_i \ne v_1, \ i \ge 2, \\ & 0 < \lambda \le s, \ 0 < t \le s/s', \ (3.7), \ (3.8), \ (3.9)\},\end{aligned}$$

then we have

$$|\mathcal{A}(s, s')| \ll V^3 + |\mathcal{A}_1(s, s')|.$$

We next make the substitutions

$$\begin{aligned} Y &= X + dv_1, \\ V_i &= v_i - v_1, \quad i \ge 2, \\ T &= t - dv_1 \mod s/s', \end{aligned} \tag{3.10}$$

so that

$$\begin{aligned} f_1(X) &= Y(Y + dV_2)(Y + dV_3) = Y^3 + d(V_2 + V_3)Y^2 + d^2V_2V_3Y \\ &= g_1(Y), \end{aligned} \tag{3.11}$$

$$\begin{aligned} f_2(X) &= (Y + dV_4)(Y + dV_5)(Y + dV_6) = Y^3 + d\sigma_1Y^2 + d^2\sigma_2Y + d^3\sigma_3 \\ &= g_2(Y), \end{aligned} \tag{3.12}$$

where

$$\begin{aligned}\sigma_1 &= V_4 + V_5 + V_6,\\ \sigma_2 &= V_4V_5 + V_4V_6 + V_5V_6,\\ \sigma_3 &= V_4V_5V_6.\end{aligned} \tag{3.13}$$

We see that (3.8) becomes

$$6(g_1(Y) + \lambda g_2(Y)) \equiv 6(1+\lambda)(Y+T)^3 \mod s. \tag{3.14}$$

The proof of the following Lemma follows that of [13, Lemma 4].

Lemma 3.10. *With notation as in* (3.10) *and* (3.13)*, consider the relations*

$$(s/s', T) = 1, \quad (s/s', T - dV_3) = 1, \tag{3.15}$$

$$6d^2T^3(V_3^2 - \sigma_1V_3 + \sigma_2) - 18d^3\sigma_3T^2 + 18d^4V_3\sigma_3T - 6d^5V_3^2\sigma_3 \equiv 0 \mod s, \tag{3.16}$$

$$6d^3\sigma_3 \equiv 0 \mod s', \tag{3.17}$$

and let

$$\begin{aligned}\mathcal{A}_2(s,s') = \{(V_3,\ V_4,\ V_5,\ V_6,\ T) \in \mathbb{Z}^5\ :\\ 0 < |V_i| \le V,\ 0 < T \le s/s',\ (3.15),\ (3.16),\ (3.17)\}.\end{aligned}$$

Then we have

$$|\mathcal{A}_1(s,s')| \ll (d,s)V(1+V/q)|\mathcal{A}_2(s,s')|.$$

Proof. We first note that (3.7) and (3.10) imply (3.15). Let

$$\begin{aligned}\mathcal{B}_1 = \{(V_2, V_3, V_4, V_5, V_6, T) \in \mathbb{Z}^6\ :\ 0 < |V_i| \le V,\\ 0 < \lambda \le s,\ (\lambda, s) = 1,\ 0 < T \le s/s', (3.9), (3.14), (3.15)\},\end{aligned}$$

so that

$$|\mathcal{A}_1(s,s')| \le V|\mathcal{B}_1|.$$

Using (3.11) and (3.12) and considering common powers of Y in (3.14) we get

$$6d(V_2 + V_3 + \lambda\sigma_1) \equiv 18(1+\lambda)T \mod s, \tag{3.18}$$

$$6d^2(v_2V_3 + \lambda\sigma_2) \equiv 18(1+\lambda)T^2 \mod s, \tag{3.19}$$

$$6d^3\lambda\sigma_3 \equiv 6(1+\lambda)T^3 \mod s. \tag{3.20}$$

By (3.18) we see that

$$6dV_2 \equiv 18(1+\lambda)T - dV_3 - d\lambda\sigma_1 \mod s,$$

which has $O\left((d,s)(1+V/q)\right)$ solutions in V_2.

The equations (3.9) and (3.20) imply that

$$6d^3\sigma_3 \equiv 0 \mod s',$$

$$6(1+\lambda) \equiv 0 \mod s',$$

and

$$6\lambda(d^3\sigma_3 - T^3) \equiv 6T^3 \mod s. \tag{3.21}$$

Combining $(T, s/s') = 1$ with the above equations implies that there are $O(1)$ possible values of λ. Finally combining (3.18), (3.19) and (3.21) gives (3.16). □

The following is [13, Lemma 2].

Lemma 3.11. *For any integer s, uniformly over all polynomials $G(X)$ with integer coefficients and fixed degree, we have*

$$|\{0 \le x < s,\ G(x) \equiv 0 \mod s,\ (s, G'(x))|6\}| \le s^{o(1)},$$

as $s \to \infty$.

The proof of the following Lemma follows that of [13, Lemma 5].

Lemma 3.12. *For $s''|(s/s')$ consider the relations*

$$(s, 6d^3\sigma_3) = s's'', \tag{3.22}$$

$$6d^2(V_3^2 - \sigma_1 V_3 + \sigma_2) \equiv 0 \mod s, \tag{3.23}$$

and let

$$\mathcal{A}_3(s,s',s'') = \{(V_3,V_4,V_5,V_6) \in \mathbb{Z}^4 \ :\ 0 < |V_i| \le V,\ (3.22),\ (3.23)\}.$$

Then we have

$$|\mathcal{A}_2(s,s')| \le s^{o(1)} \sum_{s''|s/s'} s''|\mathcal{A}_3(s,s',s'')|.$$

Proof. For $s''|(s/s')$ let

$$\mathcal{A}_3'(s,s',s'') = \{(V_3,V_4,V_5,V_6,T) \in \mathcal{A}_2(s,s') \ :\ (s, 6d^3\sigma_3) = s's''\},$$

then we have

$$|\mathcal{A}_2(s,s')| = \sum_{s''|(s/s')} |\mathcal{A}_3'(s,s',s'')|. \tag{3.24}$$

Let $S = (s', s/s')$ so that $(s'/S, s/s') = 1$. For points $(V_3, V_4, V_5, V_6, T) \in \mathcal{A}_3(s,s',s'')$ since

$$6d^3\sigma_3 \equiv 0 \mod Ss'', \tag{3.25}$$

we have by (3.15), (3.16) and (3.22)

$$6d^2(V_3^2 - \sigma_1 V_3 + \sigma_2) \equiv 0 \mod Ss''. \tag{3.26}$$

By (3.16) this implies that

$$\begin{aligned}\frac{6d^2(V_3^2 - \sigma_1 V_3 + \sigma_2)}{Ss''}T^3 - \frac{18d^3\sigma_3}{Ss''}T^2 \\ + \frac{18d^4\sigma_3 V_3}{Ss''}T - \frac{6d^5\sigma_3 V_3^2}{Ss''} \equiv 0 \mod s/(s's'').\end{aligned} \tag{3.27}$$

Let

$$G(T) = \frac{6d^2(V_3^2 - \sigma_1 V_3 + \sigma_2)}{Ss''}T^3 - \frac{18d^3\sigma_3}{Ss''}T^2 + \frac{18d^4\sigma_3 V_3}{Ss''}T - \frac{6d^5\sigma_3 V_3^2}{Ss''},$$

so that

$$3G(T) - TG'(T) = -\frac{18d^3\sigma_3}{Ss''}(T - dV_3)^2.$$

Writing $6d^3\sigma_3 = s's''\sigma'$ with $(\sigma', s) = 1$ we see from (3.15) that for some integer y with $(y, s/s') = 1$ we have

$$3G(T) - TG'(T) = -\frac{3s'}{S}y.$$

If T_0 is a root of $G(T) \pmod{s/(s's'')}$ then from $(s'/S, s/s') = 1$ we get

$$(G'(T_0), s/(s's''))|6,$$

hence by Lemma 3.11 the number of possible values for T is $\ll s''s^{o(1)}$. Finally (3.26) implies

$$6d^2(V_3^2 - \sigma_1 V_3 + \sigma_2) \equiv 0 \mod s'',$$

and the result follows from (3.24). □

Lemma 3.13. *With notation as in Lemma 3.12, for integers s, s', s'' satisfying $s'|s$ and $s''|s/s'$ we have*

$$|\mathcal{A}_3(s,s',s'')| \le (d^3, s)V^4 s^{o(1)}/(s's'').$$

Proof. Bounding the number of solutions to the equation (3.23) trivially and recalling the definition of σ_3 from (3.13) we see that

$$\begin{aligned}&|\mathcal{A}_3(s,s',s'')|\\ &\quad\le V|\{(V_4,V_5,V_6)\in\mathbb{Z}^3 : 0<|V_i|\le V,\ (s,6d^3V_4V_5V_6)=s's''\}|.\end{aligned}\tag{3.28}$$

Writing $s=(d^3,s)s_1$ and $d^3=(d^3,s)d_1$ and considering

$$(s,6d^3V_4V_5V_6)=s's'',$$

we see that

$$(s_1,6V_4V_5V_6)=s's''/(d^3,s).$$

For integers s_1,s_2,s_3, let

$$\mathcal{A}_4(s_1,s_2,s_3)=\{(V_4,V_5,V_6)\in\mathbb{Z}^3\ :\ 0<|V_i|\le V,\ s_1|6V_4,\ s_2|6V_5,\ s_3|6V_6\}.$$

From (3.28)

$$|\mathcal{A}_3(s,s',s'')|\le V\sum_{s_1s_2s_3=s's''/(d^3,s)}|\mathcal{A}_4(s_1,s_2,s_3)|,$$

and since

$$|\mathcal{A}_4(s_1,s_2,s_3)|\ll\frac{V^3}{s_1s_2s_3}=\frac{(d^3,s)V^3}{s's''},$$

we see that

$$|\mathcal{A}_3(s,s',s'')|\le\frac{(d^3,s)V^4s^{o(1)}}{s's''}.$$

□

Lemma 3.14. *Let $s'|s$ and*

$$\begin{aligned}\mathcal{A}(s,s')=\{\ \mathbf{v}\in\mathbb{Z}^6\ :\ &0<v_i\le V, \textit{there exists an } x \textit{ such that}\\ &(s,f_1(x)f_2(x))=1,\ s|F(x),\ s|F'(x),\ s'|F''(x)\}.\end{aligned}$$

Then

$$|\mathcal{A}(s,s')|\le(d,s)^4\left(\frac{V^6}{ss'}+\frac{V^5}{s'}\right)q^{o(1)}+V^3.$$

Proof. Combining Lemma 3.9, Lemma 3.10 and Lemma 3.12 we get

$$|\mathcal{A}(s,s')|\le V^3+(d,s)\left(1+\frac{V}{s}\right)V\sum_{s''|s/s'}s''|\mathcal{A}_3(s,s',s'')|.$$

Applying Lemma 3.13 to summation over s'' gives

$$\sum_{s''|s/s'} s''|\mathcal{A}_3(s,s',s'')| \leq \frac{s^{o(1)}(d^3,s)V^4}{s'}.$$

□

For integer q, we define the numbers $h_1(q), h_2(q), h_3(q)$ as in [13]

$$\begin{aligned} h_1(q)^2 &= \text{smallest square divisible by } q, \\ h_2(q)^3 &= \text{smallest cube divisible by } q, \\ h_3(q) &= \text{ product of distinct prime factors of } q. \end{aligned} \tag{3.29}$$

The following is [13, Theorem 2].

Lemma 3.15. *Let χ be a primitive character mod q and let*

$$q = q_0q_1q_2q_3, \tag{3.30}$$

where the q_i are pairwise coprime. Let the integers l_0, l_1, l_2 satisfy

$$l_0|h_1(q_0)/h_3(q_0), \quad l_1|h_2(q_1)/h_3(q_1), \quad l_2|h_2(q_2)/h_3(q_2), \tag{3.31}$$

and consider the relations

$$l_0h_1(q_1q_2q_3)|F(x), \quad (F(x), h_1(q_0)) = l_0, \tag{3.32}$$

$$l_1h_2(q_2q_3)|F'(x), \quad (F'(x), h_2(q_1)) = l_1, \tag{3.33}$$

$$l_2h_2(q_3)|F''(x), \quad (F''(x), h_2(q_2)) = l_2. \tag{3.34}$$

Letting

$$\mathcal{C} = \mathcal{C}(l_0,l_1,l_2,q_0,q_1,q_2,q_3) = \{1 \leq x \leq q \ : (3.32),\ (3.33),\ (3.34)\},$$

we have

$$\left|\sum_{x\in\mathcal{C}} \chi(f_1(x))\overline{\chi}(f_2(x))\right| \leq q^{1/2+o(1)}\frac{(q_2q_3l_1)^{1/2}l_2}{h_2(q_2)}.$$

Lemma 3.16. *For any primitive character χ mod q and any integer $V < q^{1/6}d^{-2}$ we have*

$$\sum_{v_1,\dots,v_6=1}^{V} \left|\sum_{x=1}^{q} \chi\left(\prod_{i=1}^{3}(x+dv_i)\right)\overline{\chi}\left(\prod_{i=4}^{6}(x+dv_i)\right)\right| \leq V^3q^{1+o(1)}.$$

Proof. With notation as above and in (3.5) and (3.6)

$$\sum_{v_1,\dots,v_6=1}^{V}\left|\sum_{x=1}^{q}\chi\left(\prod_{i=1}^{3}(x+dv_i)\right)\overline{\chi}\left(\prod_{i=4}^{6}(x+dv_i)\right)\right|\le\sum_{d_i,l_i}\left|\sum_{x\in\mathcal{C}}\chi(f_1(x))\overline{\chi}(f_2(x))\right|,$$

where the last sum is extended over all q_1,q_2,q_3,q_4 and l_0,l_1,l_2 satisfying the conditions of Lemma 3.15. By Lemma 3.14, for some fixed $q_1,\dots,q_4$ satisfying (3.30) and l_0,l_1,l_2 satisfying (3.31)

$$\begin{aligned}&\sum_{v_1,\dots,v_6=1}^{V}\left|\sum_{x=1}^{q}\chi\left(\prod_{i=1}^{3}(x+dv_i)\right)\overline{\chi}\left(\prod_{i=4}^{6}(x+dv_i)\right)\right|\le\\&\left((q,d)^4\left(\frac{V^6}{l_1h_2(q_2q_3)l_2h_2(q_3)}+\frac{V^5}{l_2h_2(q_3)}\right)q+V^3\right)\frac{(qq_2q_3l_1)^{1/2}l_2}{h_2(q_2)}q^{o(1)}\le\\&\left((q,d)^4V^6q^{1/2}+(q,d)^4V^5q^{2/3}+V^3q\right)q^{o(1)},\end{aligned}$$

where the last inequality follows from the definitions of l_i,h_i and q_i. The result follows since the term V^3q dominates for $V\le q^{1/6}d^{-2}$. □

Lemma 3.17. *For any primitive character χ mod q and integers M, N, d and a satisfying*

$$N\le q^{7/12}d^{-3/2},\quad d\le q^{1/12},\quad (a,q)=1,$$

we have

$$\left|\sum_{M<n\le M+N}\chi(dn+a)\right|\le q^{1/9+o(1)}d^{2/3}N^{2/3}.$$

Proof. Using the same argument from Lemma 3.7, we proceed by induction on N. Since the result is trivial for $N\le q^{1/3}$, this forms the basis of our induction. Define

$$U=[0.5Nd^2q^{-1/6}],\quad V=[0.5d^{-2}q^{1/6}],$$

and let

$$\mathcal{U}=\{\ 1\le u\le U\ :\ (u,dq)=1\ \},\quad \mathcal{V}=\{\ 1\le v\le V\ :\ (v,q)=1\ \}.$$

Fix $\varepsilon>0$, by the inductive hypothesis for any integer $h\le UV<N$ we have

$$\left|\sum_{M<n\le M+N}\chi(dn+a)\right|\le\left|\sum_{M<n\le M+N}\chi(d(n+h)+a)\right|+2q^{1/9+\varepsilon}d^{2/3}h^{2/3},$$

for sufficiently large q. Hence

$$\left|\sum_{M<n\le M+N}\chi(dn+a)\right| \le \frac{1}{|\mathcal{U}||\mathcal{V}|}|W| + 2q^{1/9+\varepsilon}d^{2/3}(UV)^{2/3},$$

where

$$W = \sum_{u\in\mathcal{U}}\sum_{v\in\mathcal{V}}\sum_{M<n\le M+N}\chi(d(n+uv)+a) = \sum_{u\in\mathcal{U}}\chi(u)\sum_{M<n\le M+N}\sum_{v\in\mathcal{V}}\chi((dn+a)u^{-1}+dv).$$

We have

$$|W| \le \sum_{x=1}^{q}\nu(x)\left|\sum_{v\in\mathcal{V}}\chi(x+dv)\right|,$$

where $\nu(x)$ counts the number of representations $x \equiv (dn+a)u^{-1} \mod q$ with $M < n \le M+N$ and $u \in \mathcal{U}$. Two applications of Hölder's inequality gives

$$|W|^6 \le \left(\sum_{x=1}^{q}\nu^2(x)\right)\left(\sum_{x=1}^{q}\nu(x)\right)^4\sum_{x=1}^{q}\left|\sum_{v\in\mathcal{V}}\chi(x+dv)\right|^6.$$

As in Lemma 3.7

$$\sum_{x=1}^{q}\nu(x) = N|\mathcal{U}|, \quad \sum_{x=1}^{q}\nu^2(x) \le \left(\frac{dNU}{q}+1\right)NUq^{o(1)}.$$

By Lemma 3.16

$$\begin{aligned}\sum_{x=1}^{q}\left|\sum_{v\in\mathcal{V}}\chi(x+dv)\right|^6 &= \sum_{v_1,\dots v_6\in\mathcal{V}}\sum_{x=1}^{q}\chi\left(\prod_{i=1}^{3}(x+dv_i)\right)\overline{\chi}\left(\prod_{i=4}^{6}(x+dv_i)\right)\\ &\le \sum_{v_1,\dots v_6=1}^{V}\left|\sum_{x=1}^{q}\chi\left(\prod_{i=1}^{3}(x+dv_i)\right)\overline{\chi}\left(\prod_{i=4}^{6}(x+dv_i)\right)\right|\\ &\le V^3q^{1+o(1)}.\end{aligned}$$

The above bounds combine to give

$$|W|^6 \le \left(\frac{dNU}{q}+1\right)NUq^{o(1)}(N|\mathcal{U}|)^4\left(V^3q\right)q^{o(1)},$$

which implies

$$\left|\sum_{M<n\le M+N}\chi(dn+a)\right| \le \left(\frac{d^{1/6}N}{V^{1/2}} + \frac{q^{1/6}N^{5/6}}{U^{1/6}V^{1/2}}\right)q^{o(1)} + 2q^{1/9+\varepsilon}d^{2/3}(UV)^{2/3}.$$

On recalling the choices of U and V we get

$$\left|\sum_{M<n\leq M+N}\chi(dn+a)\right| \leq \frac{d^{7/6}N}{q^{1/12+o(1)}} + q^{1/9+o(1)}d^{2/3}N^{2/3} + \frac{2}{5}q^{1/9+\varepsilon}d^{2/3}N^{2/3}.$$

Since

$$\frac{d^{7/6}N}{q^{1/12}} \leq q^{1/9}d^{2/3}N^{2/3} \quad \text{when} \quad dN \leq q^{13/24},$$

we have by assumption on N and d

$$\begin{aligned}\left|\sum_{M<n\leq M+N}\chi(dn+a)\right| &\leq q^{1/9+o(1)}d^{2/3}N^{2/3} + \frac{2}{5}q^{1/9+\varepsilon}d^{2/3}N^{2/3} \\ &\leq q^{1/9+\varepsilon}d^{2/3}N^{2/3},\end{aligned}$$

for sufficiently large q. □

In [26, Lemma 8] it is shown that

$$\left|\sum_{\substack{M<n\leq M+N\\(n,q)=1}}\chi(n+a)\right| \leq q^{2/21+o(1)}N^{5/7},$$

provided $N \leq q^{7/12}$. Our next Lemma can be considered as an improvement on this bound.

Lemma 3.18. *Let χ be a primitive character* mod q *and suppose $(a,q)=1$. For $N \leq q^{23/42}$ we have*

$$\left|\sum_{\substack{M<n\leq M+N\\(n,q)=1}}\chi(n+a)\right| \leq q^{1/9+o(1)}N^{2/3}.$$

Proof. We have

$$\begin{aligned}\left|\sum_{\substack{M<n\leq M+N\\(n,q)=1}}\chi(n+a)\right| &= \left|\sum_{d|q}\mu(d)\sum_{M/d<n\leq(M+N)/d}\chi(dn+a)\right| \\ &\leq \sum_{d|q}\left|\sum_{M/d<n\leq(M+N)/d}\chi(dn+a)\right|.\end{aligned}$$

Let

$$Z = \left\lfloor \frac{N^{1/3}}{q^{1/9}} \right\rfloor,$$

then by Lemma 3.7 we have

$$\sum_{d|q}\left|\sum_{M/d<n\le(M+N)/d}\chi(dn+a)\right| =$$
$$\sum_{\substack{d|q\\ d\le Z}}\left|\sum_{M/d<n\le(M+N)/d}\chi(dn+a)\right| + \sum_{\substack{d|q\\ d>Z}}\left|\sum_{M/d<n\le(M+N)/d}\chi(dn+a)\right|$$
$$\le \sum_{\substack{d|q\\ d\le Z}} q^{1/9+o(1)}N^{2/3} + \sum_{\substack{d|q\\ d>Z}}\frac{N}{d}.$$

Since by choice of Z

$$\sum_{\substack{d|q\\ d\le Z}} q^{1/9+o(1)}N^{2/3} + \sum_{\substack{d|q\\ d>Z}}\frac{N}{d} \le \left(q^{1/9}N^{2/3}+\frac{N}{Z}\right)q^{o(1)} \le q^{1/9+o(1)}N^{2/3},$$

we get the desired bound.

It remains to check that the conditions of Lemma 3.7 are satisfied. For each $d|q$ with $d \le Z$ we need

$$\frac{N}{d} \le q^{7/12}d^{-3/2}, \quad d \le q^{1/12},$$

and from the choice of Z, this is satisfied for $N \le q^{23/42}$. □

3.6 Complete Sums

The results of this section will be used to derive new bounds for bilinear character sums.

Lemma 3.19. *Let χ be a primitive character* mod q. *For integers u_1, u_2, λ we have*

$$\left|\sum_{n=1}^{q}\chi(n+u_1)\overline{\chi}(n+u_2)e^{2\pi i\lambda n/q}\right| = \left|\sum_{n=1}^{q}\chi(n+\lambda)\overline{\chi}(n)e^{2\pi i(u_1-u_2)n/q}\right|.$$

Proof. Let

$$\tau(\chi) = \sum_{n=1}^{q}\chi(n)e^{2\pi in/q},$$

be the Gauss sum, so that

$$|\tau(\chi)| = q^{1/2} \quad \text{and} \quad \sum_{n=1}^{q}\chi(n)e^{2\pi ian/q} = \overline{\chi}(a)\tau(\chi).$$

Writing

$$\chi(n+u_1) = \frac{1}{\tau(\overline{\chi})} \sum_{\lambda_1=1}^{q} \overline{\chi}(\lambda_1) e^{2\pi i(n+u_1)\lambda_1/q},$$

and

$$\overline{\chi}(n+u_1) = \frac{1}{\tau(\chi)} \sum_{\lambda_2=1}^{q} \chi(\lambda_2) e^{2\pi i(n+u_2)\lambda_2/q},$$

we have

$$\sum_{n=1}^{q} \chi(n+u_1)\overline{\chi}(n+u_2)e^{2\pi i\lambda n/q} =$$
$$\frac{1}{\tau(\chi)\tau(\overline{\chi})} \sum_{\lambda_1=1}^{q}\sum_{\lambda_2=1}^{q} \overline{\chi}(\lambda_1)e^{2\pi i\lambda_1 u_2/q}\chi(\lambda_2)e^{2\pi i\lambda_2 u_2/q} \sum_{n=1}^{q} e^{2\pi i n(\lambda+\lambda_1+\lambda_2)}.$$

Since

$$\sum_{\lambda_1=1}^{q}\sum_{\lambda_2=1}^{q} \overline{\chi}(\lambda_1)e^{2\pi i\lambda_1 u_2/q}\chi(\lambda_2)e^{2\pi i\lambda_2 u_2/q} \sum_{n=1}^{q} e^{2\pi i n(\lambda+\lambda_1+\lambda_2)} =$$
$$\chi(-1)e^{-2\pi i u_2\lambda/q} q \sum_{\lambda_1=1}^{q} \chi(\lambda_1+\lambda)\overline{\chi}(\lambda_1)e^{2\pi i\lambda_1(u_1-u_2)/q},$$

we have

$$\left|\sum_{n=1}^{q} \chi(n+u_1)\overline{\chi}(n+u_2)e^{2\pi i\lambda n/q}\right| = \frac{q}{|\tau(\chi)|^2}\left|\sum_{n=1}^{q} \chi(n+\lambda)\overline{\chi}(n)e^{2\pi i n(u_1-u_2)/q}\right|$$
$$= \left|\sum_{n=1}^{q} \chi(n+\lambda)\overline{\chi}(n)e^{2\pi i n(u_1-u_2)/q}\right|.$$

□

Lemma 3.20. *Let χ be a primitive character* mod q*. For integers b and λ with $b \not\equiv 0$* mod q *we have*

$$\left|\sum_{\substack{n=1\\(n,q)=1}}^{q} \chi\left(1+\frac{b}{n}\right) e^{2\pi i\lambda n/q}\right| \leq (b,q)q^{1/2+o(1)}.$$

Proof. Consider first when $\lambda \equiv 0 \pmod{q}$. By Lemma 3.19

$$\left|\sum_{\substack{n=1\\(n,q)=1}}^{q} \chi\left(1+\frac{b}{n}\right) e^{2\pi i\lambda n/q}\right| = \left|\sum_{n=1}^{q} |\chi(n)|^2 e^{2\pi i bn/q}\right| = \left|\sum_{\substack{n=1\\(n,q)=1}}^{q} e^{2\pi i bn/q}\right|,$$

and from [42, Equation 3.5] we have

$$\left| \sum_{\substack{n=1 \\ (n,q)=1}}^{q} e^{2\pi i b n/q} \right| \ll (b,q).$$

This gives

$$\left| \sum_{\substack{n=1 \\ (n,q)=1}}^{q} \chi\left(1+\frac{b}{n}\right) e^{2\pi i \lambda n/q} \right| \ll (b,q) \leq (b,q) q^{1/2+o(1)}.$$

Next consider when $\lambda \not\equiv 0 \pmod{q}$. We first note that if χ is a character $\bmod p$ with p prime then we have from the Weil bound (see [59, Theorem 2G])

$$\left| \sum_{\substack{n=1 \\ (n,p)=1}}^{p} \chi\left(1+\frac{b}{n}\right) e^{2\pi i \lambda n/p} \right| \ll p^{1/2}.$$

For p prime and integers λ, b, c and α we let $N(\lambda, b, c, p^\alpha)$ denote the number of solutions to the congruence

$$\lambda n^2 \equiv cb \mod p^\alpha, \quad 1 \leq n \leq p^\alpha, \quad (n,p) = 1. \tag{3.35}$$

We have

$$N(\lambda, b, c, p^\alpha) \leq 4(\lambda, p^\alpha), \tag{3.36}$$

since if there exists a solution n to (3.35) then $(\lambda, p^\alpha) = (cb, p^\alpha)$. This implies that that for some integer a with $(a,p) = 1$ we have

$$n^2 \equiv a \pmod{p^\alpha/(p^\alpha, \lambda)}. \tag{3.37}$$

The bound (3.36) follows since there are at most 4 solutions to (3.37).

Suppose $q = p^{2\alpha}$ is an even prime power and let c be defined by

$$\chi(1+p^\alpha) = e^{2\pi i c/p^\alpha}.$$

From the argument of [9, Lemma 2] (see also [42, Lemma 12.2]) we have by (3.36)

$$\left| \sum_{\substack{n=1 \\ (n,q)=1}}^{q} \chi\left(1+\frac{b}{n}\right) e^{2\pi i \lambda n/q} \right| \ll p^\alpha N(\lambda, b, c) \ll (\lambda, q) q^{1/2}.$$

Suppose next $q = p^{2\alpha+1}$ is an odd prime power with $p > 2$ and let c be defined by

$$\chi(1 + p^{\alpha+1}) = e^{2\pi i c/p^\alpha}.$$

From the argument of [9, Lemma 4] (see also [42, Lemma 12.3]) we get

$$\begin{aligned}\left|\sum_{\substack{n=1\\(n,q)=1}}^{q} \chi\left(1+\frac{b}{n}\right) e^{2\pi i\lambda n/q}\right| &\ll p^{(2\alpha+1)/2} N(\lambda, b, c, p^\alpha) + p^\alpha N(\lambda, b, c, p^{\alpha+1}) \\ &\ll (\lambda, q) q^{1/2}.\end{aligned}$$

Finally if $q = 2^{2\alpha+1}$, then from the argument of [9, Lemma 3]

$$\begin{aligned}\left|\sum_{\substack{n=1\\(n,q)=1}}^{q} \chi\left(1+\frac{b}{n}\right) e^{2\pi i\lambda n/q}\right| &\ll 2^{1/2} 2^\alpha N(\lambda, b, c, p^\alpha) \\ &\ll (\lambda, q) q^{1/2}.\end{aligned}$$

Combining the above bounds gives the desired result when q is a prime power.

For the general case, suppose χ is a primitive character $\bmod q$ and let $q = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ be the prime factorization of q. By the Chinese Remainder Theorem we have

$$\chi = \chi_1 \chi_2 \cdots \chi_k,$$

where each χ_i is a primitive character $\bmod p_i^{\alpha_i}$. Let $q_i = q/p^{\alpha_i}$. By the above bounds and another application of the Chinese remainder theorem (see [42, Equation 12.21]) we have for some absolute constant C

$$\begin{aligned}&\left|\sum_{\substack{n=1\\(n,q)=1}}^{q} \chi\left(1+\frac{b}{n}\right) e^{2\pi i\lambda n/q}\right| = \\ &\left|\sum_{\substack{n_1=1\\(n_1,p_1)=1}}^{p_1^{\alpha_1}} \cdots \sum_{\substack{n_k=1\\(n_k,p_k)=1}}^{p_k^{\alpha_k}} \chi_1\left(1+\frac{b}{\sum_{i=1}^k n_i q_i}\right) e^{2\pi i\lambda n_1/p_1^{\alpha_1}} \ldots \chi_k\left(1+\frac{b}{\sum_{i=1}^k n_i q_i}\right) e^{2\pi i\lambda n_k/p_i^{\alpha_k}}\right| \\ &= \left|\prod_{i=1}^{k}\left(\sum_{\substack{n_i=1\\(n_i,p_i)=1}}^{p_i^{\alpha_i}} \chi_i\left(1+\frac{b}{n_i q_i}\right) e^{2\pi i\lambda n_i/p_i^{\alpha_i}}\right)\right| \leq \prod_{i=1}^{k} C(\lambda, p_i^{\alpha_i}) p_i^{\alpha_i/2} \leq (\lambda, q) q^{1/2+o(1)},\end{aligned}$$

and the result follows from Lemma 3.19. □

3.7 Bilinear Character Sums

Lemma 3.21. *Let K and L be integers and for any two sequences $(\alpha_k)_{k=1}^K$ and $(\beta_\ell)_{\ell=1}^L$ of complex numbers supported on integers coprime to q and any integer a coprime to q let*

$$W = \sum_{k\le K}\sum_{\ell\le L}\alpha_k\,\beta_\ell\,\chi(k\ell+a).$$

Then we have

$$W \le \left(KL^{1/2} + (1+K^{1/2}q^{-1/2})q^{1/4}K^{1/2}L\right)q^{o(1)},$$

where

$$A = \max_{k\le K}|\alpha_k| \qquad \text{and} \qquad B = \max_{\ell\le L}|\beta_\ell|.$$

Proof. By the Cauchy-Schwarz inequality

$$\begin{aligned}|W|^2 &\le A^2K\sum_{k\le K}\left|\sum_{\ell\le L}\beta_\ell\chi(k\ell+a)\right|^2\\ &\le A^2B^2K^2L + \left|\sum_{k\le K}\sum_{\substack{\ell_1,\ell_2\le L\\ \ell_1\ne\ell_2}}\beta_{\ell_1}\overline{\beta}_{\ell_2}\chi(k\ell_1+a)\overline{\chi}(k\ell_2+a)\right|.\end{aligned}$$

Let

$$W_1 = \sum_{k\le K}\sum_{\substack{\ell_1,\ell_2\le L\\ \ell_1\ne\ell_2}}\beta_{\ell_1}\overline{\beta}_{\ell_2}\chi(k\ell_1+a)\overline{\chi}(k\ell_2+a).$$

We have

$$\begin{aligned}|W_1| &\le \frac{B^2}{q}\sum_{\substack{\ell_1<\ell_2\le L\\ (\ell_1,q)=1\\ (\ell_2,q)=1}}\left|\sum_{s=1}^{q}\sum_{k\le K}e^{-2\pi isk/q}\sum_{\lambda=1}^{q}\chi(\lambda+a\ell_1^{-1})\overline{\chi}(\lambda+a\ell_2^{-1})e^{2\pi is\lambda/q}\right|\\ &\le \frac{B^2}{q}\sum_{\substack{\ell_1<\ell_2\le L\\ (\ell_1,q)=1\\ (\ell_2,q)=1}}\sum_{s=1}^{q}\left|\sum_{k\le K}e^{-2\pi isk/q}\right|\left|\sum_{\lambda=1}^{q}\chi(\lambda+a\ell_1^{-1})\overline{\chi}(\lambda+a\ell_2^{-1})e^{2\pi is\lambda/q}\right|.\end{aligned}$$

By Lemma 3.20

$$\sum_{\substack{\ell_1<\ell_2\le L\\(\ell_1,q)=1\\(\ell_2,q)=1}}\sum_{s=1}^{q}\left|\sum_{k\le K}e^{-2\pi isk/q}\right|\left|\sum_{\lambda=1}^{q}\chi(\lambda+a\ell_1^{-1})\overline{\chi}(\lambda+a\ell_2^{-1})e^{2\pi is\lambda/q}\right|\ll$$

$$\sum_{\ell_1<\ell_2\le L}\sum_{s=1}^{q}\min\left(K,\frac{1}{||s/q||}\right)(\ell_1-\ell_2,q)q^{1/2+o(1)}.$$

Since

$$\sum_{\substack{\ell_1,\ell_2\le L\\ \ell_1\ne\ell_2}}(\ell_1-\ell_2,q)\ll\sum_{\ell\le L}\sum_{\substack{\ell_1,\ell_2\le L\\ \ell_1<\ell_2\\ \ell_1-\ell_2=\ell}}(\ell,q)\le L\sum_{d\mid q}\sum_{\substack{\ell\le L\\ d\mid\ell}}1\le L^2q^{o(1)},$$

we get

$$|W_1|\le\frac{B^2}{q}\left(\sum_{s=1}^{q}\min\left(K,\frac{1}{||s/q||}\right)\right)q^{1/2+o(1)}L^2\le B^2\left(1+\frac{K}{q}\right)q^{1/2+o(1)}L^2.$$

This implies that

$$|W|^2\le A^2B^2K\left(KL+\left(1+\frac{K}{q}\right)q^{1/2+o(1)}L^2\right).$$

□

Next, we use an idea of Garaev [30] to derive a variant of Lemma 3.21 in which the summation limits over ℓ depend on the parameter k.

Lemma 3.22. *Let K, L be natural numbers and let the sequences $(L_k)_{k=1}^K$ and $(M_k)_{k=1}^K$ of nonnegative integers be such that $M_k < L_k \le L$ for each k. For any two sequences $(\alpha_k)_{k=1}^K$ and $(\beta_\ell)_{\ell=1}^L$ of complex numbers supported on integers coprime to q and for any integer a coprime to q, let*

$$\widetilde{W}=\sum_{k\le K}\sum_{M_k<\ell\le L_k}\alpha_k\,\beta_\ell\,\chi(k\ell+a).$$

Then we have

$$\widetilde{W}\ll\left(KL^{1/2}+(1+K^{1/2}q^{-1/2})q^{1/4}K^{1/2}L\right)q^{o(1)},$$

where

$$A=\max_{k\le K}|\alpha_k|\qquad\text{and}\qquad B=\max_{\ell\le L}|\beta_\ell|.$$

Proof. For real z we denote

$$e_L(z)=\exp(2\pi iz/L).$$

Considering summation over ℓ in the definition of $\widetilde{W}$, we use the orthogonality of exponential functions to get

$$\sum_{M_k<\ell\le L_k}\beta_\ell\,\chi(k\ell+a)=\sum_{\ell\le L}\sum_{M_K<s\le L_k}\beta_\ell\,\chi(k\ell+a)\cdot\frac{1}{L}\sum_{-\frac{1}{2}L<r\le\frac{1}{2}L}e_L(r(\ell-s))$$
$$=\frac{1}{L}\sum_{-\frac{1}{2}L<r\le\frac{1}{2}L}\sum_{M_k<s\le L_k}e_L(-rs)\sum_{\ell\le L}\beta_\ell\,e_L(r\ell)\,\chi(k\ell+a).$$

In view of [42, Bound (8.6)], for each $k\le K$ and every integer r such that $|r|\le\frac{1}{2}L$ we can write

$$\sum_{M_k<s\le L_k}e_L(-rs)=\sum_{s\le L_k}e_L(-rs)-\sum_{s\le M_k}e_L(-rs)=\eta_{k,r}\frac{L}{|r|+1},$$

for some complex number $\eta_{k,r}\ll 1$.

Letting $\widetilde{\alpha}_{k,r}=\alpha_k\,\eta_{k,r}$ and $\widetilde{\beta}_{\ell,r}=\beta_\ell\,e_L(r\ell)$ we may write

$$\sum_{K_0<k\le K}\sum_{M_k<\ell\le L_k}\alpha_k\,\beta_\ell\,\chi(k\ell+a)=\sum_{-\frac{1}{2}L<r\le\frac{1}{2}L}\frac{1}{|r|+1}\sum_{k\le K}\sum_{\ell\le L}\widetilde{\alpha}_{k,r}\widetilde{\beta}_{\ell,r}\,\chi(k\ell+a).$$

Applying Lemma 3.21 with the sequences $(\widetilde{\alpha}_{k,r})_{k=1}^{K}$ and $(\widetilde{\beta}_{\ell,r})_{\ell=1}^{L}$, and noting that

$$\sum_{-\frac{1}{2}L<r\le\frac{1}{2}L}\frac{1}{|r|+1}\ll\log L,$$

we derive the stated bound. □

3.8 Proof of Theorem 3.1

Considering the sum

$$S_a(q;N)=\sum_{n\le N}\Lambda(n)\chi(n+a),$$

we apply Lemma 3.2 with

$$f(n)=\begin{cases}\chi(n+a) & \text{if}\quad (n,q)=1,\\ 0 & \text{otherwise.}\end{cases}$$

3.8.1 The sum Σ_1

For Σ_1 in Lemma 3.2 we apply the trivial estimate obtained from the Prime Number Theorem

$$\Sigma_1 = \left|\sum_{n\le U}\Lambda(n)f(n)\right| \ll U.$$

3.8.2 The sum Σ_2

We have

$$\Sigma_2 = (\log UV)\sum_{\substack{v\le UV\\(v,q)=1}}\left|\sum_{\substack{s\le N/v\\(s,q)=1}}\chi(sv+a)\right| = (\log UV)\sum_{\substack{v\le UV\\(v,q)=1}}\left|\sum_{\substack{s\le N/v\\(s,q)=1}}\chi(s+av^{-1})\right|.$$

Since $N\le q$, an application of Lemma 3.4 gives

$$\begin{aligned}\sum_{\substack{v\le Nq^{-43/72}\\(v,q)=1}}\left|\sum_{\substack{s\le N/v\\(s,q)=1}}\chi(s+av^{-1})\right| &\le \sum_{\substack{v\le Nq^{-43/72}\\(v,q)=1}} q^{1/2+o(1)}\\ &\le Nq^{-7/72+o(1)}.\end{aligned}$$

By Lemma 3.8

$$\begin{aligned}\sum_{\substack{Nq^{-43/72}<v\le Nq^{-11/24}\\(v,q)=1}}\left|\sum_{\substack{s\le N/v\\(s,q)=1}}\chi(s+av^{-1})\right| &\le q^{3/16+o(1)}N^{1/2}\left(\sum_{Nq^{-43/72}<v\le Nq^{-11/24}} v^{-1/2}\right)\\ &\le Nq^{-1/24+o(1)},\end{aligned}$$

and by Lemma 3.18

$$\begin{aligned}\sum_{\substack{Nq^{-11/24}<v\le UV\\(v,q)=1}}\left|\sum_{\substack{s\le N/v\\(s,q)=1}}\chi(s+av^{-1})\right| &\le q^{1/9+o(1)}N^{2/3}\left(\sum_{Nq^{-11/24}<v\le UV} v^{-2/3}\right)\\ &\le q^{1/9+o(1)}N^{2/3}(UV)^{1/3}.\end{aligned}$$

Combining the above bounds gives

$$\Sigma_2 \le \left(Nq^{-1/24+o(1)} + q^{1/9}N^{2/3}(UV)^{1/3}\right)q^{o(1)}.$$

3.8.3 The sum Σ_3

Arguing as above, we get

$$\Sigma_3 = (\log N) \sum_{\substack{v \le V \\ (v,q)=1}} \max_{w \ge 1} \left| \sum_{\substack{w \le s \le N/v \\ (s,q)=1}} \chi(s + av^{-1}) \right| \le \left(Nq^{-1/24+o(1)} + q^{1/9} N^{2/3} V^{1/3} \right) q^{o(1)}.$$

3.8.4 The sum Σ_4

For the sum Σ_4, we have

$$\Sigma_4 = \sum_{\substack{U < k \le \frac{N}{V} \\ \gcd(k,q)=1}} \Lambda(k) \sum_{V < \ell \le N/k} A(\ell) \chi(k\ell + a),$$

where

$$A(\ell) = \sum_{d \mid \ell,\, d \le V} \mu(d), \quad \gcd(\ell, q) = 1,$$

and

$$A(\ell) = 0, \quad \gcd(\ell, q) > 1.$$

We note that

$$\Lambda(k) \le \log k \le k^{o(1)} \qquad \text{and} \qquad |A(\ell)| \le \tau(\ell) \le \ell^{o(1)}.$$

Separating the sum Σ_4 into $O(\log N)$ sums of the form

$$W(K) = \sum_{\substack{K < k \le 2K \\ \gcd(k,q)=1}} \Lambda(k) \sum_{V < \ell \le N/k} A(\ell) \chi(k\ell + a),$$

where $U \le K \le N/V$.

By Lemma 3.22 we have

$$\begin{aligned} W(K) &\le \left(K^{1/2} N^{1/2} + (1 + K^{1/2} q^{-1/2}) q^{1/4} K^{-1/2} N \right) q^{o(1)} \\ &\le K^{1/2} N^{1/2} + q^{1/4} K^{-1/2} N + N q^{-1/4+o(1)}, \end{aligned} \tag{3.38}$$

so that summing over the $O(\log N)$ values of $U \le K \le NV^{-1}$ gives

$$\Sigma_4 \le \left(NV^{-1/2} + q^{1/4} N U^{-1/2} + N q^{-1/4} \right) (Nq)^{o(1)}.$$

3.8.5 Optimization of Parameters

Combining the estimates for $\Sigma_1, \Sigma_2, \Sigma_3$ and Σ_4 gives

$$S_a(q;N) \leq \left(Nq^{-1/24+o(1)} + U + NV^{-1/2} + q^{1/4}NU^{-1/2} + q^{1/9}N^{2/3}(UV)^{1/3}\right)(Nq)^{o(1)}.$$

We choose $U = q^{1/2}V$ to balance the terms $NV^{-1/2}$ and $q^{1/4}NU^{-1/2}$ which gives

$$S_a(q;N) \leq \left(Nq^{-1/24+o(1)} + U + NV^{-1/2} + q^{5/18}N^{2/3}V^{2/3}\right)(Nq)^{o(1)}.$$

Choosing $V = N^{2/7}q^{-5/21}$ to balance the terms $NV^{-1/2}$ and $q^{5/18}N^{2/3}V^{2/3}$ we get

$$S_a(q;N) \leq \left(Nq^{-1/24+o(1)} + q^{11/42}N^{2/7} + q^{5/42}N^{6/7}\right)(Nq)^{o(1)}.$$

We have $U \geq V \geq 1$ when $N \geq q^{5/6}$ which is when the term $q^{5/42}N^{6/7}$ becomes nontrivial.

Also we need

$$UV = q^{1/42}N^{4/7} \leq N$$

which is satisfied for $N \geq q^{1/18}$ which we may suppose since otherwise the bound is trivial. Finally we note that we may remove the middle term, since it is dominated by the last term for $N \geq q^{1/4}$.

Chapter 4

Mixed Character Sums

4.1 Introduction

4.1.1 Background

Let q be an integer, χ a primitive multiplicative character $\bmod q$ and F a polynomial of degree d with real coefficients. We consider a variety of character sums mixed with terms of the form $e^{2\pi i F(n)}$. The simplest example of such sums is given by

$$\sum_{M<n\leq N+M} \chi(n)e^{2\pi i F(n)}. \tag{4.1}$$

For prime q, these sums were first studied by Enflo [22] who outlines an argument based on Weyl differencing which gives the bound

$$|S(\chi, F)| \leq N^{1-1/2^d r} q^{(r+1)/2^{d+2}r^2+o(1)},$$

for integer $r \geq 1$ and is nontrivial provided $H > q^{1/4+\delta}$. This bound was improved by Chang [15] who showed that

$$|S(\chi, F)| \ll Nq^{-\varepsilon}, \tag{4.2}$$

provided $N \geq q^{1/4+\delta}$ and

$$\varepsilon = \frac{\delta^2}{4(1+2\delta)(2+(d+1)^2)}.$$

In the same paper Chang considers a generalisation of the sums (4.1) to arbitrary finite fields. More specifically, let q be prime, n an integer, χ and ψ multiplicative and additive characters of $\mathbb{F}_{q^n}$ respectivley and F a polynomial of degree d with coefficients in

$\mathbb{F}_{q^n}$. Let $\omega_1, \ldots, \omega_n$ be a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let $\mathcal{B}$ denote the box

$$\mathcal{B} = \{\omega_1 h_1 + \cdots + \omega_n h_n : 1 \leq h_i \leq H\}.$$

Chang showed that

$$\sum_{h \in \mathcal{B}} \chi(h)\psi(F(h)) \ll H^n q^{-\varepsilon}, \tag{4.3}$$

when $H \geq q^{1/4+\delta}$ and ε is given by

$$\varepsilon = \frac{\delta^2 n}{4(1+2\delta)(2n+(d+1)^2)}.$$

Recently, Heath-Brown and Pierce [38] have improved on the bound of Chang (4.2) for prime fields showing that, subject to some conditions on r related to Vinogradov's mean value theorem, we have

$$\left| \sum_{M < n \leq M+N} \chi(n) e^{2\pi i F(n)} \right| \leq N^{1-1/r} q^{(r+1-d(d+1)/2)/4r(r-d(d+1)/2)}. \tag{4.4}$$

The above bound can be compared directly with the result of Chang by noting that for small δ and $N \geq q^{1/4+\delta}$, we have

$$N^{1-1/r} q^{(r+1-d(d+1)/2)/4r(r-d(d+1)/2)} \leq N q^{-\varepsilon},$$

where ε behaves like (see [38, Section 4.2])

$$\varepsilon \sim \left(\frac{2\delta}{1+\sqrt{1+2d(d+1)\delta}} \right)^2 \quad \text{as} \quad \delta \to 0.$$

Pierce [53] also considers a multidimensional version of the sums (4.1). Let $q_1, \ldots, q_n$ be primes, χ_i a multiplicative character mod q_i and F a polynomial of degree d in n variables. Pierce has given a number of different bounds for sums of the form

$$\sum_{N_i < h_i \leq N_i + H_i} \chi_1(h_1) \ldots \chi_n(h_n) e^{2\pi i F(h_1, \ldots, h_n)}. \tag{4.5}$$

In the same paper, Pierce mentions the following problem. Let $L_1, \ldots, L_n$ be n linear forms in n variables which are linearly independent mod q and let F be a polynomial of degree d in n variables. Then the problem is to give an upper bound for the sums

$$\sum_{1 \leq h_i \leq H} \chi\left(\prod_{j=1}^{n} L_j(h_1, \ldots, h_n)\right) e^{2\pi i F(h_1, \ldots, h_n)}. \tag{4.6}$$

The sums (4.6) without the factor $e^{2\pi i F(h_1,\dots,h_n)}$ were first considered by Burgess [11] whose bound was later improved by Bourgain and Chang [6].

4.1.2 New Results

We first consider the problem of extending the bound of Heath-Brown and Pierce (4.4) to squarefree modulus. The main obstacle in doing this is bounding the double mean value

$$\int_0^1 \dots \int_0^1 \sum_{\lambda=1}^{q} \left| \sum_{1\le v\le V} \beta_v \chi(\lambda+v) e^{2\pi i(\alpha_1 v+\dots+\alpha_d v^d)} \right|^{2r} d\alpha_1 \dots d\alpha_d.$$

For the case of prime modulus, Heath-Brown and Pierce [38] combine the Weil bounds for complete sums with Vinogradov's mean value theorem. For the case of squarefree modulus, we can use the Chinese remainder theorem, as done by Burgess [9] for pure sums, so that we may apply the Weil bounds, although there are extra complications in incorporating bounds for Vinogradov's mean value theorem. Doing this we end up with a bound weaker than for prime modulus, although in certain cases we can get something just as sharp, in particular when q does not have many prime factors.

We give an improvement on the bound (4.2) of Chang for boxes over finite fields. We deal with the factor $\psi(F(h))$ in a similar fashion to the case of squarefree modulus. Our argument also relies on Konyagin's bound on the multiplicitive energy of boxes in finite fields [44], Vinogradov's mean value theorem and the Weil bounds for complete sums.

We show in certain cases we may improve on the results of Pierce for the sums (4.5). The argument of Pierce relies on a multidimensional version of Vinogradov's mean value theorem due to Parsell, Prendiville and Wooley [52]. Our improvement comes from averaging the sums (4.5) in a suitable way so we end up applying the classical Vinogradov mean value theorem rather than the multidimensional version. Although in order to do this, we need the range of summation in each variable not to get too short and each of the q_i in (4.5) not to be too small, so our result is less general.

Finally, we consider the problem mentioned by Pierce in [53], of bounding the sums (4.6). We obtain a result almost as strong as Bourgain and Chang [6] for the case of pure sums. An essential part of our proof is the bound of Bourgain and Chang on multiplicative energy of systems of linear forms.

4.1.3 New Arguments

Our arguments use a different approach to that of Heath-Brown and Pierce [38]. The technique we use to deal with the factor $e^{2\pi iF(n)}$ can be thought of as incorporating principles of the large sieve. We also mention a paper of Chamizo [14] who considers incomplete Gauss sums and provides inspiration for some of our ideas.

We briefly indicate our technique for dealing with mixed sums in a general setting. Let $F(x,y)$ be a polynomial of degree d with real coefficients, $\Phi(k,v)$ a sequence of complex numbers and consider the bilinear form

$$W = \sum_{1\leq k\leq K}\sum_{1\leq v\leq V}\gamma_k\beta_v\Phi(k,v)e^{2\pi iF(k,v)}.$$

Our first step is an application of the triangle inequality

$$|W| \leq \sum_{1\leq k\leq K}|\gamma_k|\left|\sum_{1\leq v\leq V}\beta_v\Phi(k,v)e^{2\pi iF(k,v)}\right|.$$

For $i=1,\dots,d$, we let

$$\delta_i = \frac{1}{4V^i},$$

and define the functions $\phi_i(v)$ by

$$1 = \phi_i(v)\int_{-\delta_i}^{\delta_i} e^{2\pi ixv^i}dx,$$

so that for $1 < v \leq V$ we have

$$\phi_i(v) = \frac{\pi iv^i}{\sin(2\pi\delta_i v^i)} \ll \frac{1}{\delta_i} \ll V^i.$$

Considering W, we have

$$\begin{aligned} W &\leq \sum_{1\leq k\leq K}|\gamma_k|\max_{\alpha_1,\dots,\alpha_d\in\mathbb{R}}\left|\sum_{1\leq v\leq V}\int_{-\delta_1}^{\delta_1}\dots\int_{-\delta_d}^{\delta_d}\prod_{i=1}^{d}\phi_i(v)\beta_v\Phi(k,v)e^{2\pi i((\alpha_1+x_1)v+\dots+(\alpha_d+x_d)v^d)}d\mathbf{x}\right| \\ &\leq \sum_{1\leq k\leq K}|\gamma_k|\max_{\alpha_1,\dots,\alpha_d\in\mathbb{R}}\int_{-\delta_1}^{\delta_1}\dots\int_{-\delta_d}^{\delta_d}\left|\sum_{1\leq v\leq V}\beta'_v\Phi(k,v)e^{2\pi i((\alpha_1+x_1)v+\dots+(\alpha_d+x_d)v^d)}\right|d\mathbf{x}, \end{aligned}$$

where

$$\beta'_v = \beta_v\prod_{i=1}^{d}\phi_i(v).$$

Applying Hölder's inequality gives

$$W^{2r} \leq V^{-(2r-1)d(d+1)/2} \left(\sum_{1 \leq k \leq K} |\gamma_k|^{2r/(2r-1)} \right)^{2r-1} \times \left(\sum_{1 \leq k \leq K} \max_{\alpha_1, \dots, \alpha_d \in \mathbb{R}} \int_{-\delta_1}^{\delta_1} \dots \int_{-\delta_d}^{\delta_d} \left| \sum_{1 \leq v \leq V} \beta_v' \Phi(k, v) e^{2\pi i((\alpha_1 + x_1)v + \dots + (\alpha_d + x_d)v^d)} \right|^{2r} d\mathbf{x} \right).$$

By extending the range of integration we may remove the condition $\max_{\alpha_1, \dots, \alpha_d \in \mathbb{R}}$, since

$$\sum_{1 \leq k \leq K} \max_{\alpha_1, \dots, \alpha_d \in \mathbb{R}} \int_{-\delta_1}^{\delta_1} \dots \int_{-\delta_d}^{\delta_d} \left| \sum_{1 \leq v \leq V} \beta_v' \Phi(k, v) e^{2\pi i((\alpha_1 + x_1)v + \dots + (\alpha_d + x_d)v^d)} \right|^{2r} d\mathbf{x} \ll \sum_{1 \leq k \leq K} \int_{[0,1]^d} \left| \sum_{1 \leq v \leq V} \beta_v' \Phi(k, v) e^{2\pi i(x_1 v + \dots + x_d v^d)} \right|^{2r} d\mathbf{x}.$$

Mean values of the form

$$\int_{[0,1]^d} \left| \sum_{1 \leq v \leq V} \beta_v' \Phi(k, v) e^{2\pi i(x_1 v + \dots + x_d v^d)} \right|^{2r} d\mathbf{x}, \tag{4.7}$$

have been considered in a number of previous works, see for example [5, 7, 8, 39, 69], and are closely related to Vinogradov's Mean Value Theorem, which we describe below.

Concerning the sums (4.7), we note that one may use results of Bourgain, Demeter and Guth [8, Theorem 4.1] based on restriction theory to show that (4.7) is bounded by

$$V^{o(1)} \left(1 + V^{r - d(d+1)/2}\right) \left(\sum_{1 \leq v \leq V} \left| \beta_v' \Phi(k, v) \right|^2 \right)^r. \tag{4.8}$$

One may then incorporate summation over k in (4.8) and use properties specific to Φ to obtain a final bound. The author does not use results from restriction theory to bound the mean values (4.7). It may be possible to improve on the results obtained in this thesis by incorporating the bound (4.8) in the methods used.

Although our approach is different to that of Heath-Brown and Pierce, we also rely on bounds for Vinogradov's mean value theorem. For integers r, d, V, we let $J_{r,d}(V)$ denote the number of solutions to the system of equations

$$v_1^i + \dots + v_r^i = v_{r+1}^i + \dots + v_{2r}^i, \quad 1 \leq i \leq d, \quad 1 \leq v_j \leq V.$$

Bounds for $J_{r,d}(V)$ are generally referred to as Vinogradov's Mean Value Theorem. Concerning bounds for $J_{r,d}(V)$, significant progress has been made by Wooley [67, 68] and very recently Bourgain, Demeter and Guth [8] have proved the main conjecture for $J_{r,d}(V)$ when $d > 3$. In particular, combining the main results of Bourgain, Demeter and Guth [8] with those of Wooley [68] for the case $d = 3$, we have for any integers r, d and V

$$J_{r,d}(V) \leq (V^r + V^{2r-d(d+1)/2})V^{o(1)}.$$

In particular if $r \geq d(d+1)/2$ then we have the following estimate

$$J_{r,d}(V) \leq V^{2r-d(d+1)/2+o(1)},$$

which will be used in what follows without further reference.

4.2 Main Results

For ease of notation we let $D = d(d+1)/2$. Our first two Theorems concern mixed sums to squarefree modulus.

Theorem 4.1. *Let q be squarefree and χ a primitive character* mod q. *Let M, N, r be integers with $r \geq D+1$ and $N \leq q^{1/2+1/4(r-D/2)}$. For any polynomial $F(x)$ of degree d with real coefficients we have*

$$\left| \sum_{M < n \leq M+N} \chi(n) e^{2\pi i F(n)} \right| \leq N^{1-1/r} q^{1/4r + D/8r(r-D/2) + 1/4r(r-D/2) + o(1)}.$$

Theorem 4.1 is slightly worse than the bound of Heath-Brown and Pierce (4.4) for prime modulus, although in certain cases we can get something almost as sharp.

Theorem 4.2. *Let s be an integer, q squarefree with at most s prime factors and χ a primitive character* mod q. *Let M, N, r be integers with $r \geq D + s + 1$ and $N \leq q^{1/2+1/4(r-D)}$. For any polynomial $F(x)$ of degree d with real coefficients we have*

$$\left| \sum_{M < n \leq M+N} \chi(n) e^{2\pi i F(n)} \right| \leq N^{1-1/r} q^{(r+1-D)/4r(r-D) + o(1)}.$$

Our next Theorem improves the bound of Chang for mixed sums in finite fields [15]. Before we state our result we introduce some notation. Let $\omega_1, \ldots, \omega_n$ be a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let F be a polynomial of degree d in n variables with real coefficients. For $x \in \mathbb{F}_{q^n}$ we define $F(x)$ by

$$F(x) = F(h_1, \ldots, h_n),$$

where

$$x = h_1\omega_1 + \cdots + h_n\omega_n.$$

Theorem 4.3. *Let q be prime, n and r integers and χ a multiplicative character of $\mathbb{F}_{q^n}$. Let $\omega_1, \ldots, \omega_n$ be a basis for $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$. For integer H let $\mathcal{B}$ denote the box*

$$\mathcal{B} = \{h_1\omega_1 + \cdots + h_n\omega_n : 0 < h_i \leq H\}.$$

Let F be a polynomial of degree d in n variables with real coefficients. Then if $r \geq D+1$ and $H \leq q^{1/2}$ we have

$$\left|\sum_{\mathbf{x}\in\mathcal{B}} \chi(\mathbf{x})e^{2\pi iF(\mathbf{x})}\right| \leq |\mathcal{B}|^{1-1/r}q^{n(r-D+1)/4r(r-D)+o(1)}.$$

We note that the sums in Theorem 4.3 are slightly more general than those considered by Chang [15], since any additive character ψ of $\mathbb{F}_{q^n}$ is of the form

$$\psi(x) = e^{2\pi i\mathrm{Tr}(ax)/q},$$

for some $a \in \mathbb{F}_{q^n}$, where $\mathrm{Tr}(z)$ is the trace of $z \in \mathbb{F}_{q^n}$ in $\mathbb{F}_q$.

Our next Theorem improves on some results of Pierce [53] in certain circumstances.

Theorem 4.4. *Let $q_1, \ldots, q_n$ be primes which may not be distinct and for each i let χ_i be a multiplicative character* mod q_i. *Let F be a polynomial of degree d in n variables with real coefficients and let $\mathcal{B}$ denote the box*

$$\mathcal{B} = \{(h_1, \ldots, h_n) : M_i < h_i \leq M_i + H_i\}.$$

For integer $r \geq D+1$, if for each i we have $q_i > q^{1/2(r-D)}$ and $q^{1/2(r-D)} \leq H_i \leq q_i^{1/2+1/4(r-D)}$ then

$$\left|\sum_{\mathbf{x}\in\mathcal{B}} \chi_1(x_1)\ldots\chi_n(x_n)e^{2\pi iF(\mathbf{x})}\right| \leq |\mathcal{B}|^{1-1/r}q^{(r-D+n)/4r(r-D)+o(1)},$$

where $q = q_1 \ldots q_n$.

Our final Theorem extends a bound of Bourgain and Chang [6] to the setting of mixed character sums.

Theorem 4.5. *Let q be prime, r an integer and χ a multiplicative character* mod q. *Let $L_1, \ldots, L_n$ be linear forms with integer coefficients in n variables which are linearly independent* mod q. *Let $\mathcal{B}$ denote the box*

$$\mathcal{B} = \{(h_1, \ldots, h_n) : 1 < h_i \leq H\},$$

and let F be a polynomial of degree d in n variables with real coefficients. Then if $r \geq D+1$ and $H \leq q^{1/2}$ we have

$$\left|\sum_{\mathbf{x}\in\mathcal{B}} \chi\left(\prod_{i=1}^{n} L_i(\mathbf{x})\right) e^{2\pi i F(\mathbf{x})}\right| \leq |\mathcal{B}|^{1-1/r} q^{n(r-D+1)/4r(r-D)+o(1)}.$$

4.3 Reduction to Multilinear Forms

The following can be thought of a multidimensional version of a technique from the proof of [28, Theorem 1].

Lemma 4.6. *Let $\mathbf{n} = (n_1, \dots, n_r)$ and $G(\mathbf{n})$ be any complex valued function on the integers. Let $\mathcal{B}$ and $\mathcal{B}_0$ denote the boxes*

$$\mathcal{B} = \{(n_1, \dots, n_r) \in \mathbb{Z}^r : 1 \leq n_i \leq N_i,\ 1 \leq i \leq r\},$$

$$\mathcal{B}_0 = \{(n_1, \dots, n_r) \in \mathbb{Z}^r : -N_i \leq n_i \leq N_i,\ 1 \leq i \leq r\}.$$

Let $U_1, \dots, U_r$ and V be positive integers such that $U_i V \leq N_i$ and let $\mathcal{U} \subset \mathbb{Z}^r$ be any set such that if $(u_1, \dots, u_r) \in \mathcal{U}$ then $1 \leq u_i \leq U_i$. For some $\alpha \in \mathbb{R}$ we have

$$\left|\sum_{\mathbf{n}\in\mathcal{B}} G(\mathbf{n})\right| \ll \frac{\log N_1 \dots \log N_r}{V|\mathcal{U}|} \sum_{\mathbf{n}\in\mathcal{B}_0} \sum_{\mathbf{u}\in\mathcal{U}} \left|\sum_{1\leq v\leq V} G(\mathbf{n}+v\mathbf{u}) e^{2\pi i \alpha v}\right|.$$

Proof. In what follows we let $\langle ., . \rangle$ denote the standard inner product on $\mathbb{R}^r$. For $\mathbf{u} \in \mathcal{U}$ and $1 \leq v \leq V$ we have

$$\sum_{\mathbf{n}\in\mathcal{B}} G(n) = \sum_{\mathbf{n}\in\mathcal{B}_0} G(\mathbf{n}+v\mathbf{u}) \sum_{\mathbf{n}\in\mathcal{B}} \int_{[0,1]^r} e\left(\langle \mathbf{b}, \mathbf{n}+v\mathbf{u}-\mathbf{m}\rangle\right) d\mathbf{b}.$$

Averaging over $1 \leq v \leq V$ and $\mathbf{u} \in \mathcal{U}$ gives

$$\sum_{\mathbf{n}\in\mathcal{B}} G(\mathbf{n}) = \frac{1}{V|\mathcal{U}|} \sum_{\mathbf{n}\in\mathcal{B}_0} \sum_{\mathbf{u}\in\mathcal{U}} \int_{[0,1]^r} e(\langle \mathbf{b}, \mathbf{n}\rangle) \sum_{1\leq v\leq V} G(\mathbf{n}+v\mathbf{u}) e(v\langle \mathbf{b}, \mathbf{u}\rangle) \sum_{\mathbf{m}\in\mathcal{B}} e(-\langle \mathbf{b}, \mathbf{m}\rangle) d\mathbf{b}.$$

This implies that

$$\left|\sum_{\mathbf{n}\in\mathcal{B}} G(\mathbf{n})\right| \leq \frac{1}{V|\mathcal{U}|} \int_{[0,1]^r} \sum_{\mathbf{n}\in\mathcal{B}_0} \sum_{\mathbf{u}\in\mathcal{U}} \left|\sum_{1\leq v\leq V} G(\mathbf{n}+v\mathbf{u}) e(v\langle \mathbf{b}, \mathbf{u}\rangle)\right| \left|\sum_{\mathbf{m}\in\mathcal{B}} e(-\langle \mathbf{b}, \mathbf{m}\rangle)\right| d\mathbf{b},$$

which is bounded by

$$\left|\sum_{\mathbf{n}\in\mathcal{B}} G(\mathbf{n})\right| \leq \frac{1}{V|\mathcal{U}|}\max_{\alpha\in\mathbb{R}}\sum_{\mathbf{n}\in\mathcal{B}_0}\sum_{\mathbf{u}\in\mathcal{U}}\left|\sum_{1\leq v\leq V} G(\mathbf{n}+v\mathbf{u})e(v\alpha)\right|\int_{[0,1]^r}\prod_{j=1}^{r}\left(\min(N_j,||b_j||^{-1})\right)d\mathbf{b}$$
$$\leq \frac{\log N_1\dots\log N_r}{V|\mathcal{U}|}\max_{\alpha\in\mathbb{R}}\sum_{\mathbf{n}\in\mathcal{B}_0}\sum_{\mathbf{u}\in\mathcal{U}}\left|\sum_{1\leq v\leq V} G(\mathbf{n}+v\mathbf{u})e(v\alpha)\right|.$$

□

4.4 Mean Value Estimates

We keep notation as in the introduction and recall that $J_{r,d}(V)$ denotes the number of solutions to the system of equations

$$v_1^i+\dots+v_r^i = v_{r+1}^i+\dots+v_{2r}^i, \quad 1\leq i\leq d, \quad 1\leq v_j\leq V.$$

The following is due to Burgess and is a special case of [9, Lemma 7]. Since the statement of Burgress is weaker than what the argument implies we reproduce the proof.

Lemma 4.7. *Let q be squarefree, χ a primitive character* mod q, $\mathbf{v}=(v_1,\dots,v_{2r})$ *be a $2r$-tuple of integers. For each integer $1\leq i\leq 2r$ define $A_i(\mathbf{v})$ by*

$$A_i(\mathbf{v}) = \prod_{\substack{j=1\\ j\neq i}}^{2r}(v_i-v_j).$$

For any $1\leq i\leq 2r$ such that $A_i(\mathbf{v})\neq 0$ we have

$$\left|\sum_{\lambda=1}^{q}\chi\left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1})\dots(\lambda+v_{2r})}\right)\right| \leq (q,A_i(\mathbf{v}))^{1/2}q^{1/2+o(1)}. \tag{4.9}$$

Proof. Let

$$q=p_1\dots p_k,$$

be the prime factorization of q. By the Chinese remainder theorem there exists primitive characters

$$\chi_j \mod p_j, \quad 1\leq j\leq k,$$

such that

$$\chi=\chi_1\dots\chi_k.$$

A second application of the Chinese remainder theorem gives

$$\sum_{\lambda=1}^{q}\chi\left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1})\dots(\lambda+v_{2r})}\right)=\prod_{j=1}^{k}\left(\sum_{\lambda=1}^{p_j}\chi_j\left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1})\dots(\lambda+v_{2r})}\right)\right).$$

From [9, Lemma 1] we have

$$\sum_{\lambda=1}^{p_j}\chi_j\left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1})\dots(\lambda+v_{2r})}\right)\ll(p_j,A_i(\mathbf{v}))^{1/2}p_j^{1/2}, \tag{4.10}$$

which by the above implies that

$$\left|\sum_{\lambda=1}^{q}\chi\left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1})\dots(\lambda+v_{2r})}\right)\right|\leq(q,A_i(\mathbf{v}))^{1/2}q^{1/2+o(1)}.$$

□

The following will be used in the proof of Theorem 4.1.

Lemma 4.8. *Let q be squarefree, χ a primitive character* mod q*, β_v be a sequence of complex numbers with $|\beta_v|\leq 1$ and let*

$$W=\int_0^1\dots\int_0^1\sum_{\lambda=1}^{q}\left|\sum_{1\leq v\leq V}\beta_v\chi(\lambda+v)e^{2\pi i(\alpha_1 v+\dots+\alpha_k v^k)}\right|^{2r}d\alpha_1\dots d\alpha_k. \tag{4.11}$$

Then we have

$$W\leq\left(qV^r+q^{1/2}J_{r,k}(V)^{1/2}V^r\right)q^{o(1)}.$$

Proof. Let $\mathcal{J}_{r,k}(V)$ denote the set of all $(v_1,\dots,v_{2r})$ such that

$$v_1^j+\dots+v_r^j=v_{r+1}^j+\dots+v_{2r}^j,\quad 1\leq j\leq k,\quad 1\leq v_i\leq V.$$

Expanding the $2r$-th power in the definition of W and interchanging summation and integration gives

$$W\leq\sum_{(v_1,\dots,v_{2r})\in\mathcal{J}_{r,k}(V)}\left|\sum_{\lambda=1}^{q}\chi\left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1}\dots(\lambda+v_{2r})}\right)\right|.$$

We break $\mathcal{J}_{r,k}(V)$ into sets $\mathcal{J}'_{r,k}(V)$ and $\mathcal{J}''_{r,k}(V)$, where

$$\mathcal{J}'_{r,k}(V)=\{(v_1,\dots,v_{2r})\in\mathcal{J}_{r,k}(V):\text{at least } r+1 \text{ of } v_1,\dots,v_{2r} \text{ are distinct}\},$$
$$\mathcal{J}''_{r,k}(V)=\{(v_1,\dots,v_{2r})\in\mathcal{J}_{r,k}(V):(v_1,\dots,v_{2r})\notin\mathcal{J}'_{r,k}(V)\},$$

so that $|\mathcal{J}''_{r,k}(V)| \ll V^r$. Considering $\mathcal{J}'_{r,k}(V)$, since at least $r+1$ of the v_j are distinct there exists an i such that $A_i(\mathbf{v}) \neq 0$. An application of Lemma 4.7 gives

$$W \ll qV^r + q^{1/2+o(1)} \left(\sum_{i=1}^{2r} \sum_{\substack{(v_1,\dots,v_{2r}) \in \mathcal{J}'_{r,k}(V) \\ A_i(\mathbf{v}) \neq 0}} (A_i(\mathbf{v}), q)^{1/2} \right).$$

For $1 \leq i \leq 2r$ let

$$W_i = \sum_{\substack{(v_1,\dots,v_{2r}) \in \mathcal{J}'_{r,k}(V) \\ A_i(\mathbf{v}) \neq 0}} (A_i(\mathbf{v}), q)^{1/2},$$

so that an application of the the Cauchy-Schwarz inequality gives

$$\begin{aligned} W_i &\leq \left(\sum_{(v_1,\dots,v_{2r}) \in \mathcal{J}'_{r,k}(V)} 1 \right)^{1/2} \left(\sum_{\substack{(v_1,\dots,v_{2r}) \\ A_i(\mathbf{v}) \neq 0}} (A_i(\mathbf{v}), q) \right)^{1/2} \\ &\leq |\mathcal{J}_{r,k}(V)|^{1/2} \left(\sum_{\substack{v_1,\dots,v_{2r} \\ A_i(\mathbf{v}) \neq 0}} (A_i(\mathbf{v}), q) \right)^{1/2}. \end{aligned}$$

For the last sum, we have

$$\sum_{\substack{(v_1,\dots,v_{2r}) \\ A_i(\mathbf{v}) \neq 0}} (A_i(\mathbf{v}), q) \ll \sum_{d|q} d \sum_{\substack{A \neq 0 \\ d|A}} \sum_{\substack{v_1,\dots,v_{2r} \\ A_i(\mathbf{v}) = A}} 1.$$

We next fix a value of A and consider $(v_1, \dots, v_{2r})$ such that

$$A_i(\mathbf{v}) = A.$$

Since

$$A_i(\mathbf{v}) = \prod_{\substack{j=1 \\ j \neq i}}^{2r} (v_i - v_j),$$

we see that there are $q^{o(1)}$ choices for the numbers $(v_i - v_1), \dots, (v_i - v_{2r})$ and choosing v_i determines $v_1, \dots, v_{2r}$, uniquely. Since there are V choices for v_i and each $A_i(\mathbf{v}) \ll V^{2r-1}$

we get

$$\sum_{\substack{(v_1,\dots,v_{2r})\\ A_i(\mathbf{v})\neq 0}} (A_i(\mathbf{v}),q) \ll q^{o(1)} \sum_{d|q} d \sum_{\substack{1\le A\ll V^{2r-1}\\ d|A}} V$$
$$\ll q^{o(1)} V^{2r} \sum_{d|q} 1 = q^{o(1)} V^{2r}.$$

This gives

$$W \le \left(qV^r + q^{1/2}|\mathcal{J}_{r,k}(V)|^{1/2}V^r\right) q^{o(1)} = \left(qV^r + q^{1/2}J_{r,k}(V)^{1/2}V^r\right) q^{o(1)}.$$

□

The following will be used in the proof of Theorem 4.2 and improves on Lemma 4.8 provided the number of prime factors of q is bounded.

Lemma 4.9. *Let s be an integer and q a squarefree number such that the number of prime factors of q is less than s. Let χ be a primitive character* mod q*, β_v any sequence of complex numbers with $|\beta_v| \le 1$ and for $r \ge s+1$ let*

$$W = \int_0^1 \dots \int_0^1 \sum_{\lambda=1}^{q} \left| \sum_{1\le v\le V} \beta_v \chi(\lambda+v) e^{2\pi i(\alpha_1 v+\dots+\alpha_k v^d)} \right|^{2r} d\alpha_1 \dots d\alpha_d. \tag{4.12}$$

Then we have

$$W \le \left(qV^r + q^{1/2}J_{r-s-1,d}(V)V^{2s+2}\right) q^{o(1)}.$$

Proof. We keep the same notation from the proof of Lemma 4.8 so that

$$W \ll qV^r + q^{1/2+o(1)} \left(\sum_{i=1}^{2r} W_i\right),$$

with

$$W_i = \sum_{\substack{(v_1,\dots,v_{2r})\in\mathcal{J}'_{r,k}(V)\\ A_1(\mathbf{v})\neq 0}} (A_i(\mathbf{v}),q)^{1/2}. \tag{4.13}$$

We consider only W_1, the same argument applies to the remaining W_i.

Let $q = q_1 \dots q_s$ be the prime factorization of q. For each subset $\mathcal{S} \subseteq \{1,\dots,s\}$ we consider a partition of $\mathcal{S}$ into $2r-1$ sets

$$\mathcal{S} = \bigcup_{j=2}^{2r} U_j, \quad \text{where} \quad U_i \cap U_j = \emptyset \quad \text{if} \quad i \neq j, \tag{4.14}$$

and some U_j may be empty. We have

$$W_1 \leq \sum_{\mathcal{S}\subseteq\{1,\dots,s\}} \sum_{U_2,\dots,U_{2r}} \sum_{\substack{(v_1,\dots,v_{2r})\in\mathcal{J}'_{r,k}(V)\\ A_1(\mathbf{v})\neq 0\\ (q,v_1-v_j)=\prod_{\ell\in U_j} q_\ell}} (A_1(\mathbf{v}),q)^{1/2}, \tag{4.15}$$

where summation over $U_2,\dots,U_{2r}$ satisfies (4.14). Hence it is sufficient to show that for fixed $\mathcal{S}$ and fixed $U_2,\dots,U_{2r}$ satisfying (4.14) we have

$$\sum_{\substack{(v_1,\dots,v_{2r})\in\mathcal{J}'_{r,k}(V)\\ A_1(\mathbf{v})\neq 0\\ (q,v_1-v_j)=\prod_{\ell\in U_j} q_\ell}} (A_1(\mathbf{v}),q)^{1/2} \leq J_{r-s-1,k}(V)V^{2s+2}q^{o(1)}.$$

Considering values of j such that $U_j \neq \emptyset$, each value of v_1 determines v_j with $\ll V/\prod_{i\in U_j} q_i$ possibilities. Since there are are most s values of j such that $U_j \neq \emptyset$, we may choose two sets $\mathcal{V}_1, \mathcal{V}_2$ such that

$$\mathcal{V}_1 \subseteq \{1,\dots,r\}, \quad |\mathcal{V}_1| = r-s-1,$$

$$\mathcal{V}_2 \subseteq \{r+1,\dots,2r\}, \quad |\mathcal{V}_2| = r-s-1,$$

and

$$U_j = \emptyset, \quad \text{whenever} \quad j \in \mathcal{V}_1 \cup \mathcal{V}_2.$$

For such a selection there exists integers $\alpha_1,\dots,\alpha_k$ such that

$$\sum_{\substack{(v_1,\dots,v_r)\in\mathcal{J}'_{r,k}(V)\\ A_1(\mathbf{v})\neq 0\\ (q,v_1-v_j)=\prod_{i\in U_j} q_i}} (A_1(\mathbf{v}),q)^{1/2} \leq$$

$$\left(\sum_{\substack{1\leq v_i\leq V\\ i\notin\mathcal{V}_1\cup\mathcal{V}_2\\ A_1(\mathbf{v})\neq 0\\ (q,v_1-v_j)=\prod_{i\in U_j} q_i}} \left(\prod_{\substack{j=2\\ j\notin\mathcal{V}_1\cup\mathcal{V}_2}}^{2r} (v_1-v_j), q \right)^{1/2} \right) J(\mathcal{V}_1,\mathcal{V}_2,\alpha_1,\dots,\alpha_k),$$

where $J(\mathcal{V}_1,\mathcal{V}_2,\alpha_1,\dots,\alpha_k)$ denotes the number of solutions to the system of equations

$$\sum_{j\in\mathcal{V}_1} v_j^i - \sum_{j\in\mathcal{V}_2} v_j^i = \alpha_i, \quad 1\leq i\leq d, \quad 1\leq v_j\leq V.$$

This implies that

$$\sum_{\substack{(v_1,\dots,v_r)\in\mathcal{J}'_{r,k}(V)\\ A_1(\mathbf{v})\neq 0\\ (q,v_1-v_j)=\prod_{i\in U_j}q_i}} (A_1(\mathbf{v}),q)^{1/2} \ll V^{2s+2}J(\mathcal{V}_1,\mathcal{V}_2,\alpha_1,\dots,\alpha_k),$$

Since $J(\mathcal{V}_1,\mathcal{V}_2,\alpha_1,\dots,\alpha_k)\leq J_{r-s-1,d}(V)$, we see that

$$\sum_{\substack{(v_1,\dots,v_{2r})\in\mathcal{J}'_{r,k}(V)\\ A_1(\mathbf{v})\neq 0\\ (q,v_1-v_j)=\prod_{i\in U_j}q_i}} (A_1(\mathbf{v}),q)^{1/2} \leq V^{2s+2}J_{r-s-1,d}(V).$$

This gives

$$W_1 \leq V^{2s+2}J_{r-s-1,d}(V)q^{o(1)},$$

which combined with the above completes the proof. □

Lemma 4.10. *Let $q_1,\dots,q_n$ be primes, χ_i a multiplicative character* mod q_i*, β_v a sequence of complex numbers with $|\beta_v|\leq 1$ and let*

$$W=\int_0^1\dots\int_0^1\sum_{\substack{\lambda_i=1\\ 1\leq i\leq n}}^{q_i}\left|\sum_{1\leq v\leq V}\beta_v\prod_{i=1}^{n}\chi_i(\lambda_i+v)e^{2\pi i(\alpha_1 v+\dots+\alpha_k v^k)}\right|^{2r}d\alpha_1\dots d\alpha_k. \tag{4.16}$$

If for each i we have $V\leq q_i$, then

$$W\leq\left(qV^r+q^{1/2}J_{r,k}(V)\right)q^{o(1)},$$

where $q=q_1\dots q_n$ and the $o(1)$ term depends on n.

Proof. With notation as in the proof of Lemma 4.8, following the same argument gives

$$W\ll qV^r+\left(\sum_{(v_1,\dots,v_{2r})\in\mathcal{J}'_{r,k}(V)}\prod_{i=1}^{n}\left|\sum_{\lambda=1}^{q_i}\chi_i\left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1})\dots(\lambda+v_{2r})}\right)\right|\right).$$

We claim that if $(v_1,\dots,v_{2r})\in\mathcal{J}'_{r,k}(V)$ then for each $1\leq i\leq n$ the function

$$\chi_i\left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1})\dots(\lambda+v_{2r})}\right),$$

is not constant.

Supposing for some i this were false and letting d denote the order of χ_i, this implies that the rational function

$$\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1})\dots(\lambda+v_{2r})},$$

is a d-th power mod q_i. Hence at most $r+1$ of the $v_1, \dots, v_{2r}$ are distinct mod q_i. Since $V < q_i$ this implies that at most $r+1$ of the $v_1, \dots, v_{2r}$ are distinct, contradicting the definition of $\mathcal{J}'_{r,k}(V)$. Hence from the Weil bound for complete character sums [59, Theorem 2C', pg 43] we have

$$\sum_{\lambda=1}^{q_i} \chi_i \left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1})\dots(\lambda+v_{2r})} \right) \ll q_i^{1/2},$$

provided $(v_1, \dots, v_{2r}) \in \mathcal{J}'_{r,k}(V)$. This implies that

$$W \ll qV^r + q^{1/2+o(1)}|\mathcal{J}'_{r,k}(V)| = (qV^r + q^{1/2}J_{r,d}(V))q^{o(1)}.$$

□

Lemma 4.11. *Let q be prime, n an integer and χ a multiplicative character of $\mathbb{F}_{q^n}$, β_v any sequence of complex numbers satisfying $|\beta_v| \le 1$ and let*

$$W = \int_{[0,1]^d} \sum_{\lambda \in \mathbb{F}_{q^n}} \left| \sum_{1 \le v \le V} \beta_v \chi(\lambda+v) e^{2\pi i(\alpha_1 v_1 + \dots + \alpha_d v^d)} \right|^{2r} d\alpha_1 \dots d\alpha_d.$$

For any integer r we have

$$W \ll q^n V^r + q^{n/2} J_{r,d}(V),$$

where the implied constant depends on n.

Proof. Arguing as in the proof of Lemma 4.8, let $\mathcal{J}_{r,k}(V)$ denote the set of all $(v_1, \dots, v_{2r})$ such that

$$v_1^j + \dots + v_r^j = v_{r+1}^j + \dots + v_{2r}^j, \quad 1 \le j \le k, \quad 1 \le v_i \le V.$$

Expanding the $2r$-th power in the definition of W and interchanging summation and integration gives

$$W \le \sum_{(v_1,\dots,v_{2r}) \in \mathcal{J}_{r,k}(V)} \left| \sum_{\lambda=1}^{q} \chi \left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1}\dots(\lambda+v_{2r})} \right) \right|.$$

As in Lemma 4.8 we break the $\mathcal{J}_{r,k}(V)$ into sets $\mathcal{J}'_{r,k}(V)$ and $\mathcal{J}''_{r,k}(V)$, where

$$\mathcal{J}'_{r,k}(V) = \{(v_1, \dots, v_{2r}) \in \mathcal{J}_{r,k}(V) : \text{at least } r+1 \text{ of the } v_i's \text{ are distinct}\},$$
$$\mathcal{J}''_{r,k}(V) = \{(v_1, \dots, v_{2r}) \in \mathcal{J}_{r,k}(V) : (v_1, \dots, v_{2r}) \notin \mathcal{J}'_{r,k}(V)\}.$$

This gives

$$W \ll q^n V^r + \sum_{(v_1,\dots,v_{2r})\in\mathcal{J}'_{r,k}(V)} \left| \sum_{\lambda=1}^{q} \chi\left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1}\dots(\lambda+v_{2r})} \right) \right|.$$

From [59, Theorem 2C', pg 43], if $(v_1,\dots,v_{2r}) \in \mathcal{J}'_{r,k}(V)$ then

$$\sum_{\lambda=1}^{q} \chi\left(\frac{(\lambda+v_1)\dots(\lambda+v_r)}{(\lambda+v_{r+1}\dots(\lambda+v_{2r})} \right) \ll q^{n/2},$$

so that

$$W \ll q^n V^r + \sum_{(v_1,\dots,v_{2r})\in\mathcal{J}'_{r,k}(V)} q^{n/2}.$$

The result follows since $|\mathcal{J}'_{r,k}(V)| \le J_{r,d}(V)$. □

4.5 Multiplicative Equations

The following follows from the proof of [26, Lemma 7].

Lemma 4.12. *Let M, N, U, q be integers with*

$$NU \le q,$$

and let $\mathcal{U}$ denote the set

$$\mathcal{U} = \{\ 1 \le u \le U\ :\ (u,q) = 1\ \}.$$

The number of solutions to the congruence

$$n_1 u_1 \equiv n_2 u_2 \mod q, \quad M < n_1, n_2 \le M+N, \quad u_1, u_2 \in \mathcal{U},$$

is bounded by $NUq^{o(1)}$.

The following is due to Konyagin [44, Lemma 1].

Lemma 4.13. *Let q be prime and let $\omega_1,\dots,\omega_n \in \mathbb{F}_{q^n}$ be a basis for $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ denote the boxes*

$$\mathcal{B}_1 = \{h_1\omega_1 + \dots + h_n\omega_n : 1 \le h_i \le H\},$$

$$\mathcal{B}_2 = \{h_1\omega_1 + \dots + h_k\omega_n : 1 \le h_i \le U\},$$

and suppose that $H, U \le p^{1/2}$. *Then the number of solutions to the equation*

$$n_1 u_1 = n_2 u_2, \quad n_1, n_2 \in \mathcal{B}_1, \quad u_1, u_2 \in \mathcal{B}_2,$$

is bounded by $O\left((UH)^n \log q\right)$.

The following is due to Bourgain and Chang [6].

Lemma 4.14. *Let* q *be prime,* $L_1(\mathbf{x}), \dots, L_n(\mathbf{x})$ *be linear forms in* n *variables which are linearly independent* $\bmod q$ *and let* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *denote the boxes*

$$\mathcal{B}_1 = \{\mathbf{h} = (h_1, \dots, h_n) : 1 \le h_i \le H\},$$

$$\mathcal{B}_2 = \{\mathbf{h} = (h_1, \dots, h_n) : 1 \le h_i \le U\}.$$

If $H, U \le p^{1/2}$ *the number of solutions to the system of congruences*

$$L_i(\mathbf{x}_1)L_i(\mathbf{x}_2) \equiv L_i(\mathbf{x}_3)L_i(\mathbf{x}_4) \mod q, \quad \mathbf{x}_1, \mathbf{x}_3 \in \mathcal{B}_1, \quad \mathbf{x}_2, \mathbf{x}_4 \in \mathcal{B}_2, \quad 1 \le i \le n,$$

is bounded by $(NH)^n p^{o(1)}$.

4.6 Proof of Theorem 4.1

We define the integers

$$U = \left\lfloor \frac{N}{q^{1/2(r-d(d+1)/4)}} \right\rfloor, \quad V = \lfloor q^{1/2(r-d(d+1)/4)} \rfloor, \tag{4.17}$$

and the set

$$\mathcal{U} = \{\ 1 \le u \le U : (u, q) = 1\},$$

so that

$$|\mathcal{U}| = Uq^{o(1)}. \tag{4.18}$$

By Lemma 4.6 we have

$$\left| \sum_{M < n \le M+N} \chi(n) e^{2\pi i F(n)} \right| \le \frac{q^{o(1)}}{|\mathcal{U}|V} \sum_{M-N < n \le M+N} \sum_{u \in \mathcal{U}} \left| \sum_{1 \le v \le V} \chi(n+uv) e^{2\pi i F(n+uv)} e^{2\pi i \alpha v} \right|,$$

for some $\alpha \in \mathbb{R}$. Let

$$W = \sum_{M-N<n\le M+N} \sum_{u\in\mathcal{U}} \left| \sum_{1\le v\le V} \chi(n+uv) e^{2\pi i F(n+uv)} e^{2\pi i \alpha v} \right|. \tag{4.19}$$

Then since the polynomial F has degree d we see that

$$\begin{aligned} W &\le \sum_{M-N<n\le M+N} \sum_{u\in\mathcal{U}} \max_{(\alpha_1,\dots,\alpha_d)\in[0,1]^d} \left| \sum_{1\le v\le V} \chi(n+uv) e^{2\pi i(\alpha_1 v+\cdots+\alpha_d v^d)} \right| \\ &= \sum_{\lambda=1}^{q} I(\lambda) \max_{(\alpha_1,\dots,\alpha_d)\in[0,1]^d} \left| \sum_{1\le v\le V} \chi(\lambda+v) e^{2\pi i(\alpha_1 v+\cdots+\alpha_d v^d)} \right|, \end{aligned}$$

where $I(\lambda)$ denotes the number of solutions to the congruence

$$nu^* \equiv \lambda \pmod q, \quad M-N < n \le M+N, \quad u \in \mathcal{U}.$$

For $j = 1, \dots, d$, let

$$\delta_j = \frac{1}{4V^j},$$

and define the functions $\phi_j(v)$ by

$$1 = \phi_j(v) \int_{-\delta_j}^{\delta_j} e^{2\pi i x v^j}\, dx.$$

For $1 < v \le V$ we have

$$\phi_j(v) = \frac{\pi v^j}{\sin(2\pi\delta_j v^j)} \ll \frac{1}{\delta_j} \ll V^j. \tag{4.20}$$

Let

$$\boldsymbol{\alpha} = (\alpha_1, \dots \alpha_d), \quad \mathbf{x} = (x_1, \dots, x_d), \quad \mathbf{v} = (v, \dots, v^d),$$

and let $\mathcal{C}(\delta)$ denote the rectangle

$$[-\delta_1, \delta_1] \times \cdots \times [-\delta_d, \delta_d].$$

We have

$$W \le \sum_{\lambda=1}^{q} I(\lambda) \max_{\boldsymbol{\alpha}\in[0,1]^d} \left| \sum_{v\le V} \left(\prod_{i=1}^{d} \phi_i(v) \right) \int_{\mathcal{C}(\delta)} \chi(\lambda+v) e^{2\pi i <\boldsymbol{\alpha}+\mathbf{x},\mathbf{v}>} d\mathbf{x} \right|,$$

where $< . , . >$ denotes the standard inner product on $\mathbb{R}^d$. An application of the triangle inequality gives

$$W \leq \sum_{\lambda=1}^{q} I(\lambda) \max_{\boldsymbol{\alpha}\in[0,1]^d} \int_{\mathcal{C}(\delta)} \left| \sum_{v\leq V} \left(\prod_{i=1}^{d} \phi_i(v) \right) \chi(\lambda+v) e^{2\pi i <\boldsymbol{\alpha}+\mathbf{x},\mathbf{v}>} \right| d\mathbf{x}.$$

Two applications of the Hölder inequality give

$$|W|^{2r} \ll \left(\prod_{i=1}^{d} \delta_i \right)^{2r-1} \left(\sum_{\lambda=1}^{q} I(\lambda) \right)^{2r-2} \left(\sum_{\lambda=1}^{q} I(\lambda)^2 \right) \times$$
$$\left(\sum_{\lambda=1}^{q} \max_{\boldsymbol{\alpha}\in[0,1]^d} \int_{\mathcal{C}(\delta)} \left| \sum_{v\leq V} \left(\prod_{i=1}^{d} \phi_i(v) \right) \chi(\lambda+v) e^{2\pi i <\boldsymbol{\alpha}+\mathbf{x},\mathbf{v}>} \right|^{2r} d\mathbf{x} \right).$$

We have

$$\sum_{\lambda=1}^{q} I(\lambda) \ll NU,$$

and the term

$$\sum_{\lambda=1}^{q} I(\lambda)^2,$$

is equal to the number of solutions to the congruence

$$n_1 u_1 \equiv n_2 u_2 \mod q, \quad M - N \leq n_1, n_2 \leq M + N, \quad u_1, u_2 \in \mathcal{U}. \tag{4.21}$$

Since $0 \notin \mathcal{U}$, the number of solutions to (4.21) with $n_1 n_2 \equiv 0 \mod q$ is $\ll U^2$ and for the remaining solutions we apply of Lemma 4.12. This gives

$$\sum_{\lambda=1}^{q} I(\lambda)^2 \ll NUq^{o(1)} + U^2 \ll NUq^{o(1)}.$$

By the above, we may bound W by

$$W^{2r} \leq \left(\prod_{i=1}^{d} \delta_i \right)^{2r-1} (NU)^{2r-1} q^{o(1)} W_1,$$

where

$$W_1 = \sum_{\lambda=1}^{q} \max_{\boldsymbol{\alpha}\in[0,1]^d} \int_{\mathcal{C}(\delta)} \left| \sum_{v\leq V} \left(\prod_{i=1}^{d} \phi_i(v) \right) \chi(\lambda+v) e^{2\pi i <\boldsymbol{\alpha}+\mathbf{x},\mathbf{v}>} \right|^{2r} d\mathbf{x}.$$

Recalling the choice of δ_i we get

$$W^{2r} \leq V^{-(2r-1)d(d+1)/2} (NU)^{2r-1} q^{o(1)} W_1. \tag{4.22}$$

We have

$$W_1 = \sum_{\lambda=1}^{q} \max_{\boldsymbol{\alpha}\in[0,1]^d} \int_{\mathcal{C}(\delta)+\boldsymbol{\alpha}} \left| \sum_{v\le V} \left(\prod_{i=1}^{d} \phi_i(v) \right) \chi(\lambda+v) e^{2\pi i <\mathbf{x},\mathbf{v}>} \right|^{2r} d\mathbf{x}$$
$$\ll \sum_{\lambda=1}^{q} \int_{[0,1]^d} \left| \sum_{v\le V} \left(\prod_{i=1}^{d} \phi_i(v) \right) \chi(\lambda+v) e^{2\pi i <\mathbf{x},\mathbf{v}>} \right|^{2r} d\mathbf{x}.$$

By (4.20), for each $1 \le v \le V$ we have

$$\prod_{i=1}^{d} \phi_i(v) \ll V^{d(d+1)/2},$$

hence by Lemma 4.8

$$W_1 \ll V^{rd(d+1)} \left(qV^r + q^{1/2} V^{2r-d(d+1)/4} \right) q^{o(1)}.$$

An application of (4.19) gives

$$\left| \sum_{M<n\le M+N} \chi(n) e^{2\pi i F(n)} \right|^{2r} \le \frac{(NU)^{2r-1} \left(qV^r + q^{1/2} V^{2r-d(d+1)/4} \right) V^{d(d+1)/2} q^{o(1)}}{U^{2r} V^{2r}}.$$

Recalling the choices of U and V we get

$$\left| \sum_{M<n\le M+N} \chi(n) e^{2\pi i F(n)} \right|^{2r} \le N^{2r-2} q^{1/2+d(d+1)/8(r-d(d+1)/4)+1/2(r-d(d+1)/4)+o(1)}.$$

4.7 Proof of Theorem 4.2

Let

$$U = \left\lfloor \frac{N}{q^{1/2(r-d(d+1)/2)}} \right\rfloor, \quad V = \lfloor q^{1/2(r-d(d+1)/2)} \rfloor,$$

and let $\phi_i(v)$ be defined as in the proof of Theorem 4.1. Following the proof of Theorem 4.1 we get

$$\left| \sum_{M<n\le M+N} \chi(n) e^{2\pi i F(n)} \right|^{2r} = \frac{V^{-(2r-1)d(d+1)/2} (NU)^{2r-1}}{V^{2r} U^{2r}} W_1 q^{o(1)},$$

where

$$W_1 = \sum_{\lambda=1}^{q} \int_{[0,1]^d} \left| \sum_{v\le V} \left(\prod_{i=1}^{d} \phi_i(v) \right) \chi(\lambda+v) e^{2\pi i (x_1 v + \cdots + x_d v^d)} \right|^{2r} d\mathbf{x}.$$

By Lemma 4.9 we have

$$W_1 \ll V^{rd(d+1)}(qV^r + qV^{2r-d(d+1)/2})q^{o(1)},$$

which implies

$$\left|\sum_{M<n\le M+N}\chi(n)e^{2\pi iF(n)}\right|^{2r} \le V^{d(d+1)/2}\frac{(NU)^{2r-1}}{U^{2r}V^{2r}}\left(qV^r + q^{1/2}V^{2r-d(d+1)/2}\right)q^{o(1)}.$$

Recalling the choice of U, V gives

$$\left|\sum_{M<n\le M+N}\chi(n)e^{2\pi iF(n)}\right|^{2r} \le N^{2r-2}q^{(r+1-d(d+1)/2)/2(r-d(d+1)/2)+o(1)}.$$

4.8 Proof of Theorem 4.3

We define the numbers U and V by

$$U = \left\lfloor \frac{H}{q^{n/2(r-d(d+1)/2)}} \right\rfloor, \quad V = \lfloor q^{n/2(r-d(d+1)/2)} \rfloor.$$

In order to apply Lemma 4.6, we identify subsets of

$$\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]^n,$$

with subsets of $\mathbb{F}_{q^n}$ via

$$\mathbf{z} = (z_1, \dots, z_n) \longleftrightarrow z_1\omega_1 + \cdots + z_n\omega_n.$$

An application of Lemma 4.6 gives

$$\left|\sum_{\mathbf{x}\in\mathcal{B}}\chi(\mathbf{x})e^{2\pi iF(\mathbf{x})}\right| \le \frac{q^{o(1)}}{VU^n}\sum_{\mathbf{x}\in\mathcal{B}_0}\sum_{\mathbf{u}\in\mathcal{U}}\left|\sum_{1\le v\le V}\chi(\mathbf{x}+\mathbf{u}v)e^{2\pi iF(\mathbf{x}+\mathbf{u}v)+2\pi i\alpha v}\right|,$$

where

$$\mathcal{B}_0 = \{x_1\omega_1 + \cdots + x_n\omega_n : -H \le x_i \le H, \quad 1 \le i \le n\}.$$

Let

$$W = \sum_{\mathbf{x}\in\mathcal{B}_0}\sum_{\mathbf{u}\in\mathcal{U}}\left|\sum_{1\le v\le V}\chi(\mathbf{x}+\mathbf{u}v)e^{2\pi iF(\mathbf{x}+\mathbf{u}v)+2\pi i\alpha v}\right|. \tag{4.23}$$

Expanding $F(\mathbf{x}+\mathbf{u}v)$ as a polynomial in v gives

$$F(\mathbf{x}+\mathbf{u}v) = \sum_{i=0}^{d} F_i(\mathbf{x},\mathbf{u})v^i,$$

for some real numbers $F_i(\mathbf{x},\mathbf{u})$. This gives

$$\begin{aligned} W &\le \sum_{\mathbf{x}\in\mathcal{B}_0}\sum_{\mathbf{u}\in\mathcal{U}} \max_{(\alpha_1,\ldots,\alpha_d)\in\mathbb{R}^d} \left|\sum_{1\le v\le V} \chi(\mathbf{x}+\mathbf{u}v)e^{2\pi i(\alpha_1 v+\cdots+\alpha_d v^d)}\right| \\ &= \sum_{\lambda\in\mathbb{F}_{q^n}} I(\lambda) \max_{(\alpha_1,\ldots,\alpha_d)\in\mathbb{R}^d} \left|\sum_{1\le v\le V} \chi(\lambda+v)e^{2\pi i(\alpha_1 v+\cdots+\alpha_d v^d)}\right|, \end{aligned}$$

where $I(\lambda)$ denotes the number of solutions to the equation in $\mathbb{F}_{q^n}$

$$\mathbf{x}\mathbf{u}^{-1} = \lambda, \quad \mathbf{x}\in\mathcal{B}_0, \quad \mathbf{u}\in\mathcal{U}.$$

With $\phi_i(v)$, δ_i and $\mathcal{C}(\delta)$ as in the proof of Theorem 4.1, we let $\mathbf{v} = (v,\ldots,v^d)$. We have

$$W \le \sum_{\lambda\in\mathbb{F}_{q^n}} I(\lambda) \max_{\alpha\in\mathbb{R}^d} \int_{\mathcal{C}(\delta)} \left|\sum_{1\le v\le V}\prod_{i=1}^{d} \phi_i(v)\chi(\lambda+v)e^{2\pi i<\alpha+\mathbf{y},\mathbf{v}>}\right| d\mathbf{y}.$$

Two applications of Hölder's inequality gives

$$\begin{aligned} W^{2r} \le V^{-(2r-1)d(d+1)/2} &\left(\sum_{\lambda\in\mathbb{F}_{q^n}} I(\lambda)\right)^{2r-2} \left(\sum_{\lambda\in\mathbb{F}_{q^n}} I(\lambda)^2\right) \\ &\times \left(\sum_{\lambda\in\mathbb{F}_{q^n}} \max_{\alpha\in\mathbb{R}^d} \int_{\mathcal{C}(\delta)} \left|\sum_{1\le v\le V}\prod_{i=1}^{d} \phi_i(v)\chi(\lambda+v)e^{2\pi i<\alpha+\mathbf{y},\mathbf{v}>}\right|^{2r} d\mathbf{y}\right). \end{aligned}$$

We have

$$\sum_{\lambda\in\mathbb{F}_{q^n}} I(\lambda) \ll (HU)^n.$$

The term

$$\sum_{\lambda\in\mathbb{F}_{q^n}} I(\lambda)^2,$$

is equal to the number of solutions to the equation over $\mathbb{F}_{q^n}$

$$\mathbf{x}_1\mathbf{u}_1 = \mathbf{x}_2\mathbf{u}_2, \quad \mathbf{x}_1,\mathbf{x}_2\in\mathcal{B}_0, \quad \mathbf{u}_1,\mathbf{u}_2\in\mathcal{U}. \tag{4.24}$$

Consider first solutions to (4.24) with $\mathbf{x}_1\mathbf{x}_2 = 0$. Since $0 \notin \mathcal{U}$ we must have $\mathbf{x}_1 = \mathbf{x}_2 = 0$ and for these values there are U^{2n} solutions in variables $\mathbf{u}_1, \mathbf{u}_2$. For the remaining solutions we apply Lemma 4.13 to get

$$\sum_{\lambda \in \mathbb{F}_q} I(\lambda)^2 \leq (HU)^n q^{o(1)} + U^{2n}.$$

Since $U < H$ we have

$$W^{2r} \leq V^{-(2r-1)d(d+1)/2} (HU)^{(2r-1)n} q^{o(1)} W_1,$$

where

$$W_1 = \sum_{\lambda \in \mathbb{F}_q} \max_{\alpha \in \mathbb{R}^d} \int_{\mathcal{C}(\delta)} \left| \sum_{1 \leq v \leq V} \prod_{i=1}^{d} \phi_i(v) \chi(\lambda + v) e^{2\pi i <\alpha + \mathbf{y}, \mathbf{v}>} \right|^{2r} d\mathbf{y}.$$

We have

$$\begin{aligned} W_1 &= \sum_{\lambda \in \mathbb{F}_q} \max_{\alpha \in \mathbb{R}^d} \int_{\mathcal{C}(\delta)+\alpha} \left| \sum_{1 \leq v \leq V} \prod_{i=1}^{d} \phi_i(v) \chi(\lambda + v) e^{2\pi i <\mathbf{y}, \mathbf{v}>} \right|^{2r} d\mathbf{y} \\ &\ll \sum_{\lambda \in \mathbb{F}_q} \int_{[0,1]^d} \left| \sum_{1 \leq v \leq V} \prod_{i=1}^{d} \phi_i(v) \chi(\lambda + v) e^{2\pi i <\mathbf{y}, \mathbf{v}>} \right|^{2r} d\mathbf{y}, \end{aligned}$$

hence by Lemma 4.11 we get

$$W_1 \ll V^{rd(d+1)} \left(q^n V^r + q^{n/2} V^{2r - d(d+1)/2} \right).$$

This implies that

$$\left| \sum_{\mathbf{x} \in \mathcal{B}} \chi(\mathbf{x}) e^{2\pi i F(\mathbf{x})} \right|^{2r} \leq V^{d(d+1)/2} \frac{(HU)^{(2r-1)n}}{V^{2r} U^{2rn}} \left(q^n V^r + q^{n/2} V^{2r - d(d+1)/2} \right) q^{o(1)},$$

which on recalling the choices of U, V gives

$$\left| \sum_{\mathbf{x} \in \mathcal{B}} \chi(\mathbf{x}) e^{2\pi i F(\mathbf{x})} \right|^{2r} \leq H^{(2r-2)n} q^{(nr - nd(d+1)/2)/2(r - d(d+1)/2) + o(1)}.$$

4.9 Proof of Theorem 4.4

Let $q = q_1 \dots q_n$ and define the integers

$$V = \lfloor q^{1/2(r-d(d+1)/2)} \rfloor, \quad U_i = \left\lfloor \frac{H_i}{q^{1/2(r-d(d+1)/2)}} \right\rfloor.$$

Let $\mathcal{U}$ denote the box

$$\mathcal{U} = \{(u_1, \dots, u_n) : 1 \le u_i \le U_i\}.$$

By Lemma 4.6 we have for some $\alpha \in \mathbb{R}$

$$\left|\sum_{\mathbf{x}\in\mathcal{B}} \chi_1(x_1)\dots\chi_n(x_n)e^{2\pi iF(\mathbf{x})}\right| \le$$
$$\frac{q^{o(1)}}{VU_1\dots U_n}\sum_{\mathbf{x}\in\mathcal{B}_0}\sum_{\mathbf{u}\in\mathcal{U}}\left|\sum_{1\le v\le V}\chi_1(x_1+u_1v)\dots\chi_n(x_n+u_nv)e^{2\pi i(F(\mathbf{x}+\mathbf{u}v)+\alpha v)}\right|.$$

Writing

$$W = \sum_{\mathbf{x}\in\mathcal{B}_0}\sum_{\mathbf{u}\in\mathcal{U}}\left|\sum_{1\le v\le V}\chi_1(x_1+u_1v)\dots\chi_n(x_n+u_nv)e^{2\pi i(F(\mathbf{x}+\mathbf{u}v)+\alpha v)}\right|,$$

and letting $I(\lambda_1, \dots, \lambda_n)$ denote the number of solutions to the system of congruences

$$x_iu_i^{-1} \equiv \lambda_i \mod q_i, \quad N_i - H_i < x_i \le N_i + H_i, 1 \le u_i \le U_i, \quad 1 \le i \le n,$$

we see that

$$W \le \sum_{\substack{\lambda_i=1\\1\le i\le n}}^{q_i} I(\lambda_1,\dots,\lambda_n)\left|\sum_{1\le v\le V}\chi_1(\lambda_1+v)\dots\chi_n(\lambda_n+v)e^{2\pi i(F(\mathbf{x}+\mathbf{u}v)+\alpha v)}\right|$$
$$\le \sum_{\substack{\lambda_i=1\\1\le i\le n}}^{q_i} I(\lambda_1,\dots,\lambda_n)\max_{\alpha_1,\dots,\alpha_d\in\mathbb{R}}\left|\sum_{1\le v\le V}\chi_1(\lambda_1+v)\dots\chi_n(\lambda_n+v)e^{2\pi i(\alpha_1v+\dots+\alpha_dv^d)}\right|.$$

With notation as in the proof of Theorem 4.1, we have

$$W \le \sum_{\substack{\lambda_i=1\\1\le i\le n}}^{q_i}\max_{\boldsymbol{\alpha}\in[0,1]^d}\int_{\mathcal{C}(\delta)} I(\lambda_1,\dots,\lambda_n)$$
$$\times\left|\sum_{1\le v\le V}\left(\prod_{i=1}^{d}\phi_i(v)\right)\chi_1(\lambda_1+v)\dots\chi_n(\lambda_n+v)e^{2\pi i<\boldsymbol{\alpha}+\mathbf{x},\mathbf{v}>}\right|d\mathbf{x}.$$

Two applications of Hölder's inequality give

$$W^{2r} \le V^{-(2r-1)d(d+1)/2}\left(\sum_{\substack{\lambda_i=1\\1\le i\le n}}^{q_i} I(\lambda_1,\dots,\lambda_n)\right)^{2r-2}\left(\sum_{\substack{\lambda_i=1\\1\le i\le n}}^{q_i} I(\lambda_1,\dots,\lambda_n)^2\right)W_1,$$

where

$$W_1 = \sum_{\substack{\lambda_i=1\\1\le i\le n}}^{q_i} \max_{\boldsymbol{\alpha}\in[0,1]^d} \int_{\mathcal{C}(\delta)} \left| \sum_{1\le v\le V} \left(\prod_{i=1}^{d} \phi_i(v)\right) \chi_1(\lambda_1+v)\dots\chi_n(\lambda_n+v) e^{2\pi i<\boldsymbol{\alpha}+\mathbf{x},\mathbf{v}>} \right|^{2r} d\mathbf{x}.$$

Arguing as in the proof of Theorem 4.1 gives

$$W_1 \ll \sum_{\substack{\lambda_i=1\\1\le i\le n}}^{q_i} \int_{[0,1]^d} \left| \sum_{1\le v\le V} \left(\prod_{i=1}^{d} \phi_i(v)\right) \chi(\lambda+v) e^{2\pi i(x_1 v+\dots+x_d v^d)} \right|^{2r} d\mathbf{x},$$

which combined with by Lemma 4.10 gives

$$W_1 \le V^{rd(d+1)} \left(qV^r + q^{1/2}V^{2r-d(d+1)/2}\right) q^{o(1)}.$$

We have

$$\sum_{\substack{\lambda_i=1\\1\le i\le n}}^{q_i} I(\lambda_1,\dots,\lambda_n) \ll H_1\dots H_n U_1\dots U_n.$$

The term

$$\sum_{\substack{\lambda_i=1\\1\le i\le n}}^{q_i} I(\lambda_1,\dots,\lambda_n)^2,$$

is equal to the number of solutions to the system of equations

$$x_{i,1}u_{i,1} \equiv x_{i,2}u_{i,2} \mod q_i,$$

with

$$N_i - H_i < x_{i,1}, x_{i,2} \le N_i + H_i, \quad 1 \le u_{i,1}, u_{i,2} \le U_i, \quad 1 \le i \le n.$$

Arguing as in the proof of Theorem 4.1, an application of Lemma 4.12 gives

$$\sum_{\substack{\lambda_i=1\\1\le i\le n}}^{q_i} I(\lambda_1,\dots,\lambda_n)^2 \le (H_1U_1q_n^{o(1)} + U_1^2)(H_nU_nq_n^{o(1)} + U_n^2) \le H_1\dots H_nU_1\dots U_nq^{o(1)}.$$

The above bounds combine to give

$$\left|\sum_{\mathbf{x}\in\mathcal{B}} \chi_1(x_1)\dots\chi_n(x_n)e^{2\pi iF(\mathbf{x})}\right|^{2r} \le V^{d(d+1)/2}\frac{(H_1\dots H_n)^{2r-1}}{V^{2r}U_1\dots U_n}\left(qV^r + q^{1/2}V^{2r-d(d+1)/2}\right)q^{o(1)},$$

which on recalling the choices of $V, U_1, \ldots, U_n$, we get

$$\left|\sum_{\mathbf{x}\in\mathcal{B}} \chi_1(x_1)\ldots\chi_n(x_n)e^{2\pi iF(\mathbf{x})}\right|^{2r} \leq (H_1\ldots H_n)^{2r-2}q^{(r-d(d+1)/2+n)/2(r-d(d+1)/2)+o(1)}.$$

4.10 Proof of Theorem 4.5

We define the integers

$$U = \left\lfloor \frac{N}{q^{1/2(r-d(d+1)/2)}} \right\rfloor, \quad V = \lfloor q^{1/2(r-d(d+1)/2)} \rfloor,$$

and let $\mathcal{U}$ and let denote the set

$$\mathcal{U} = \{\mathbf{u} = (u_1, \ldots, u_n) : 1 \leq u_i \leq U\}.$$

Since z By Lemma 4.6 we have

$$\left|\sum_{\mathbf{x}\in\mathcal{B}} \chi\left(\prod_{i=1}^{n} L_i(\mathbf{x})\right) e^{2\pi iF(\mathbf{x})}\right| \leq \frac{q^{o(1)}}{VU^n} \sum_{\mathbf{x}\in\mathcal{B}_0}\sum_{\mathbf{u}\in\mathcal{U}} \left|\sum_{1\leq v\leq V} \chi\left(\prod_{i=1}^{n} L_i(\mathbf{x}+\mathbf{u}v)\right) e^{2\pi i(F(\mathbf{x})+\alpha v)}\right|.$$

Since each L_i is linear this gives

$$\left|\sum_{\mathbf{x}\in\mathcal{B}} \chi\left(\prod_{i=1}^{n} L_i(\mathbf{x})\right) e^{2\pi iF(\mathbf{x})}\right| \leq \frac{q^{o(1)}}{VU^n} W,$$

where

$$W = \sum_{\mathbf{x}\in\mathcal{B}_0}\sum_{\mathbf{u}\in\mathcal{U}} \left|\sum_{1\leq v\leq V} \chi\left(\prod_{i=1}^{n} (L_i(\mathbf{x})L_i(\mathbf{u})^{-1} + v)\right) e^{2\pi i(F(\mathbf{x})+\alpha v)}\right|.$$

Let $I(\lambda_1, \ldots, \lambda_n)$ denote the number of solutions to the system of equations

$$L_i(\mathbf{x})L_i^{-1}(\mathbf{u}) \equiv \lambda_i \mod q, \quad \mathbf{x} \in \mathcal{B}_0, \quad \mathbf{u} \in \mathcal{U}, \quad 1 \leq i \leq n.$$

Applying techniques from the preceding arguments gives

$$W^{2r} \leq V^{-(2r-1)d(d+1)/2} \left(\sum_{\lambda_i=1}^{q} I(\lambda_1, \dots, \lambda_n) \right)^{2r-2} \left(\sum_{\lambda_i=1}^{q} I(\lambda_1, \dots, \lambda_n)^2 \right)$$
$$\left(\sum_{\lambda_i=1}^{q} \int_{[0,1]^d} \left| \sum_{1 \leq v \leq V} \left(\prod_{i=1}^{d} \phi_i(v) \right) \chi\left((\lambda_1 + v) \dots (\lambda_n + v) \right) e^{2\pi i (x_1 v + \dots + x_d v^d)} \right|^{2r} d\mathbf{x} \right).$$

We have

$$\sum_{\lambda=1}^{q} I(\lambda) \ll (HU)^n.$$

By Lemma 4.14

$$\sum_{\lambda=1}^{q} I(\lambda)^2 \leq (HU)^n q^{o(1)} + U^{2n} \leq (HU)^n q^{o(1)},$$

and by Lemma 4.10

$$\sum_{\lambda=1}^{q} \int_{[0,1]^d} \left| \sum_{1 \leq v \leq V} \left(\prod_{i=1}^{d} \phi_i(v) \right) \chi(\lambda + v) e^{2\pi i (x_1 v + \dots + x_d v^d)} \right|^{2r} d\mathbf{x}$$
$$\ll V^{rd(d+1)} \left(q^n V^r + q^{n/2} V^{2r - d(d+1)/2} \right).$$

The above bounds combine to give

$$\left| \sum_{\mathbf{x} \in \mathcal{B}} \chi \left(\prod_{i=1}^{n} L_i(\mathbf{x}) \right) e^{2\pi i F(\mathbf{x})} \right|^{2r} \leq V^{d(d+1)/2} \frac{H^{(2r-1)n}}{V^{2r} U^n} \left(q^n V^r + q^{n/2} V^{2r - d(d+1)/2} \right).$$

Recalling the choice of U and V gives

$$\left| \sum_{\mathbf{x} \in \mathcal{B}} \chi \left(\prod_{i=1}^{n} L_i(\mathbf{x}) \right) e^{2\pi i F(\mathbf{x})} \right|^{2r} \leq H^{(2r-2)n} q^{n(r-D+1)/2(r-D)+o(1)}.$$

Chapter 5

The Fourth Moment of Character Sums

5.1 Introduction

For q prime and a sequence of intervals $\mathcal{I} = \{\mathcal{I}_i\}_{i=1}^4$ we consider estimating $N(\mathcal{I})$, the number of solutions to the congruence

$$x_1x_2 \equiv x_3x_4 \mod q \quad \text{with} \quad x_i \in \mathcal{I}_i. \tag{5.1}$$

The sharpest estimate for $N(\mathcal{I})$ is due to Ayyad, Cochrane and Zheng [1, Theorem 1], who obtain the asymptotic formula

$$N(\mathcal{I}) = \frac{\prod_{i=1}^4 |\mathcal{I}_i|}{q} + O\left(\log^2 q \prod_{i=1}^4 |\mathcal{I}_i|^{1/2}\right), \tag{5.2}$$

where $|\mathcal{I}_i|$ denotes the length of $\mathcal{I}_i$.

Ayyad, Cochrane and Zheng also show that in certain cases one may remove a power of $\log q$ in (5.2) at the expense of replacing the asymptotic formula with upper and lower bounds. In particular Ayyad, Cochrane and Zheng show that [1, Equation 6] if either

$$|\mathcal{I}_1| = |\mathcal{I}_2| \quad \text{and} \quad |\mathcal{I}_3| = |\mathcal{I}_4|,$$

or

$$|\mathcal{I}_1| = |\mathcal{I}_3|, \quad \text{and} \quad |\mathcal{I}_2| = |\mathcal{I}_4|,$$

then we have

$$\frac{\prod_{i=1}^{4}|\mathcal{I}_i|}{q}+\log q\prod_{i=1}^{4}|\mathcal{I}_i|^{1/2}\ll N(\mathcal{I})\ll\frac{\prod_{i=1}^{4}|\mathcal{I}_i|}{q}+\log q\prod_{i=1}^{4}|\mathcal{I}_i|^{1/2}, \tag{5.3}$$

and if

$$\prod_{i=1}^{4}|\mathcal{I}_i|\leq q^2\log^2 q,$$

then we have

$$N(\mathcal{I})\ll\log q\prod_{i=1}^{4}|\mathcal{I}_i|^{1/2}. \tag{5.4}$$

The error in the approximation for $N(\mathcal{I})$ is connected to the 4-th moment of multiplicative character sums when

$$\mathcal{I}_1=\mathcal{I}_2=\mathcal{I}_3=\mathcal{I}_4,$$

through the identity

$$N(\mathcal{I})-\frac{\prod_{i=1}^{4}|\mathcal{I}_i|}{q-1}=\frac{1}{q-1}\sum_{\chi\neq\chi_0}\left|\sum_{x\in\mathcal{I}_1}\chi(x)\right|^4. \tag{5.5}$$

By considering certain averages on the left hand side of (5.5) one may remove the log factor completely in the error term in (5.2). For example, Burgess [12] has shown that

$$\frac{1}{q}\sum_{z=1}^{q}\left(\frac{1}{q-1}\sum_{\chi\neq\chi_0}\left|\sum_{x=z+1}^{z+N}\chi(x)\right|^4\right)\ll N^2,$$

and Montgomery and Vaughan [48] have shown

$$\frac{1}{q-1}\sum_{\chi\neq\chi_0}\max_{N}\left|\sum_{x=1}^{N}\chi(x)\right|^4\ll q^2. \tag{5.6}$$

We refer the reader to Friedlander and Iwaniec [27], Harman [29] and Vaughan [66] for analytic techniques for estimating the sums (5.5) which apply for general modulus q although are restricted to intervals starting from the origin. Cochrane and Sih [18] have extended the argument of [1] to deal with composite modulus and arbitrary intervals and Friedlander and Iwaniec [28] obtain the upper bound (5.4) when $\mathcal{I}_1=\mathcal{I}_3$, $\mathcal{I}_2=\mathcal{I}_4$ and $\mathcal{I}_1$ starts from the origin.

In [1] the question is raised whether it is possible to remove a power of $\log q$ in (5.2). By (5.3) such an estimate would be sharpest possible up to implied constants. Progress in this direction has been made by Garaev and Garcia [31] who improve on (5.2) under certain conditions on the lengths of the intervals occuring in $\mathcal{I}$. The precise range of values

of $|\mathcal{I}_1|, |\mathcal{I}_2|, |\mathcal{I}_3|$ and $|\mathcal{I}_4|$ for which Garaev and Garcia's bound holds depends on values of the products obtained by multiplying distinct pairs of each $|\mathcal{I}_i|$ together and does not improve on (5.2) in general. For example, in the simplest case of $|\mathcal{I}_1| = |\mathcal{I}_2| = |\mathcal{I}_3| = |\mathcal{I}_4|$, Garaev and Garcia's bound extends (5.2) to the range $|\mathcal{I}_1| \leq q^{1/2} e^{c \log^{1/2} q}$. The aim of the current paper is to improve on (5.2) for arbitrary intervals $\mathcal{I}_i$.

We also mention that Cilleruelo and Zumalacarregui [17] have given a result which allows the saving of a logarithmic factor in congruence problems under very general conditions and is also based on ideas from Cilleruelo [16] and Garaev [29].

5.2 Main results

Theorem 5.1. *Let q be prime and $\mathcal{I} = \{\mathcal{I}_i\}_{i=1}^4$ be a sequence of intervals not containing 0 mod q. Then we have*

$$N(\mathcal{I}) = \frac{\prod_{i=1}^4 |\mathcal{I}_i|}{q} + O\left(\log q \prod_{i=1}^4 |\mathcal{I}_i|^{1/2}\right).$$

From Theorem 5.1 we immediately deduce.

Theorem 5.2. *Let q be prime and N and H integers such that the interval $[H, N+H]$ does not contain 0 mod q. Then we have*

$$\frac{1}{q-1} \sum_{\chi \neq \chi_0} \left| \sum_{H \leq n \leq H+N} \chi(n) \right|^4 \ll N^2 \log q.$$

We note that Theorem 5.2 implies Theorem 5.1 by the Hölder inequality, although we are unable to prove Theorem 5.2 directly as our argument relies on certain averaging which reduces to the case where at least two of the $\mathcal{I}_i$ have different length.

We also note that from Theorem 5.2 one may obtain sharp bounds for the number of solutions to related congruences. For example, we have the following Corollary.

Corollary 5.3. *Let $\mathcal{I}$ be as in Theorem 5.1, let $k = (k_1, k_2, k_3, k_4) \in \mathbb{Z}^4$ and $a \in \mathbb{Z}$ satisfy*

$$(k_1 k_2 k_3 k_4, q-1) = 1 \quad \text{and} \quad (a, q) = 1,$$

and let $N(\mathcal{I}, k, a)$ denote the number of solutions to the congruence

$$x_1^{k_1} x_2^{k_2} x_3^{k_3} x_4^{k_4} \equiv a \mod q \quad \text{with} \quad x_i \in \mathcal{I}_i.$$

Then we have

$$N(\mathcal{I},k,a)=\frac{\prod_{i=1}^{4}|\mathcal{I}_i|}{q}+O\left(\log q\prod_{i=1}^{4}|\mathcal{I}_i|^{1/2}\right).$$

5.3 Preliminary Definitions

The letter q always denotes a prime number. For

$$X=\{X_i\}_{i=1}^{4}\quad\text{and}\quad H=\{H_i\}_{i=1}^{4},$$

with each $X,H\in\mathbb{Z}^4$ we let $J(X,H)$ denote the number of solutions to the congruence

$$x_1x_2\equiv x_3x_4\mod q,\quad H_i\le x_i\le H_i+X_i,\quad 1\le i\le 4.$$

For $V>0$ and X and H as above we let $J_1(X,H,V)$ denote the number of solutions to the congruence

$$x_1(x_2+v)\equiv x_3x_4\mod q,\quad 1\le v\le V,\quad H_i\le x_i\le H_i+X_i,\quad 1\le i\le 4.$$

For $U>0$ and X,H and V as above we let $J_2(X,H,V,U)$ denote the number of solutions to the congruence

$$x_1(x_2+v)\equiv x_3(x_4+u)\mod q,$$
$$1\le v\le V,\quad 1\le u\le U,\quad H_i\le x_i\le H_i+X_i,\quad 1\le i\le 4.$$

Although $J(X,H)$ is essentially $N(\mathcal{I})$, we find it convenient to introduce this extra notation since our argument relates $N(\mathcal{I})$ to J_1 and J_2.

In what follows we will always assume any interval does not contain 0 mod q.

5.4 Bounds for Multiplicative Equations

In this section we state bounds for $J(X,H)$ which are due to Ayyad, Cochrane and Zheng [1] and will be used in the proof of Theorem 5.1.

The following is [1, Theorem 1].

Lemma 5.4. *For q prime and X and H as above we have*

$$J(X,H)=\frac{X_1X_2X_3X_4}{q}+O\left((X_1X_2X_3X_4)^{1/2}\log^2 q\right).$$

The following is [1, Lemma 3].

Lemma 5.5. *For q prime and X and H as above we have*

$$J(X,H) \ll \frac{X_1X_2X_3X_4}{q} + (q + X_1X_2\log q)^{1/2}\,(q + X_3X_4\log q)^{1/2}\,.$$

Moreover, the inequality holds if the products X_1X_2 and X_3X_4 are replaced by any other pairing of the X_i.

5.5 Bounds for Averaged Multiplicative Equations

The results of this section are based on techniques from [1] and [31].

Lemma 5.6. *If*

$$X_1 = X_4, \quad X_2 = X_3 \quad \textit{and} \quad V < X_2/2, \tag{5.7}$$

we have

$$J_1(X,H,V) = \frac{X_1X_2X_3X_4V}{q} + O\left(VX_2X_4\log q\log\left(X_2/V\right)\right),$$

and if

$$X_1 = X_4, \quad X_2 = X_3, \quad V < X_2/2 \quad \textit{and} \quad U < X_4/2, \tag{5.8}$$

we have

$$J_2(X,H,V,U) = \frac{X_1X_2X_3X_4UV}{q} + O\left(UVX_2X_4\left(\log\left(X_4/U\right)\log\left(X_2/V\right) + \log q\right)\right).$$

Proof. We consider only $J_2(X,H,V,U)$, a similar argument with less technical details applies to $J_1(X,H,V)$. Let $A(x)$ denote the indicator function of the set

$$\{x_4 + u \;:\; H_4 \le x_4 \le H_4 + X_4, \quad 1 \le u \le U\},$$

counted with multiplicity and considered as a subset of $\mathbb{Z}/q\mathbb{Z}$. Expanding A into a Fourier series

$$A(x) = \sum_{y=0}^{q-1} \frac{a(y)}{q} e_q(xy),$$

we see that the Fourier coefficients $a(y)$ satisfy (see for example the proof of [31, Theorem 1])

$$a(0) = X_4U, \quad a(y) \ll \min\left(X_4, \frac{1}{||y/q||}\right)\min\left(U, \frac{1}{||y/q||}\right). \tag{5.9}$$

We have

$$\begin{aligned}J_2(X,H,V,U) &= \sum_{\substack{H_i\le x_i\le H_i+X_i\\1\le i\le 3}}\sum_{1\le v\le V} A(x_1x_3^{-1}(x_2+v))\\ &= \frac{X_1X_2X_3X_4UV}{q}\\ &+\frac{1}{q}\sum_{y=1}^{q-1}a(y)\sum_{\substack{H_1\le x_1\le H_1+X_1\\H_3\le x_3\le H_3+X_3}}\sum_{\substack{H_2\le x_2\le H_2+X_2\\1\le v\le V}} e_q(yx_1x_3^{-1}(x_2+v))\\ &= \frac{X_1X_2X_3X_4UV}{q}\\ &+\frac{1}{q}\sum_{y=1}^{q-1}\sum_{z=1}^{q-1}a(y)\sum_{H_2\le x_2\le H_2+X_2}e_q(zx_2)\sum_{1\le v\le V}e_q(zv)\sum_{\substack{H_1\le x_1\le H_1+X_1\\H_3\le x_3\le H_3+X_3\\x_1y\equiv x_3z \mod q}}1.\end{aligned}$$

Let W be defined by

$$\left|J_2(X,H,V,U)-\frac{X_1X_2X_3X_4UV}{q}\right| = \frac{1}{q}W,$$

and let

$$\begin{aligned}G_1(y) &= \min\left(X_2,\frac{1}{||y/q||}\right)\min\left(V,\frac{1}{||y/q||}\right),\\ G_2(z) &= \min\left(X_4,\frac{1}{||z/q||}\right)\min\left(U,\frac{1}{||z/q||}\right).\end{aligned}$$

Combining (5.9) with the above gives

$$W \le \sum_{y=1}^{q-1}\sum_{z=1}^{q-1}G_1(y)G_2(z)\sum_{\substack{H_1\le x_1\le H_1+X_1\\H_3\le x_3\le H_3+X_3\\x_1y\equiv x_3z \mod q}}1. \tag{5.10}$$

For integers $k,j\ge 1$ we define the intervals $\mathcal{K}(k)$ and $\mathcal{J}(j)$ by

$$\mathcal{K}(k)=\left(\frac{(e^{k-1}-1)q}{X_2},\frac{(e^k-1)q}{X_2}\right],\quad \mathcal{J}(j)=\left(\frac{(e^{j-1}-1)q}{X_4},\frac{(e^j-1)q}{X_4}\right],$$

so that if $|y|\in\mathcal{K}(k)$ and $|z|\in\mathcal{J}(j)$ we have

$$G_1(y)\ll\frac{X_2}{e^k}\min\left(V,\frac{X_2}{e^k}\right),\quad G_2(z)\ll\frac{X_4}{e^j}\min\left(U,\frac{X_4}{e^j}\right).$$

In (5.10) we partition summation according to $\mathcal{K}(k)$ and $\mathcal{J}(j)$. This gives

$$\begin{aligned} W &\leq \sum_{\substack{1\leq k\ll \log X_2\\ 1\leq j\ll \log X_4}} \sum_{|y|\in\mathcal{K}(k)} \sum_{|z|\in\mathcal{J}(j)} G_1(y)G_2(z) \sum_{\substack{H_1\leq x_1\leq H_1+X_1\\ H_3\leq x_3\leq H_3+X_3\\ x_1y\equiv x_3z \mod q}} 1 \\ &\ll X_2X_4 \sum_{\substack{1\leq k\ll \log X_2\\ 1\leq j\ll \log X_4}} \frac{\min\left(V, \frac{X_2}{e^k}\right)\min\left(U, \frac{X_4}{e^j}\right)}{e^{k+j}} \sum_{|y|\in\mathcal{K}(k)} \sum_{|z|\in\mathcal{J}(j)} \sum_{\substack{H_1\leq x_1\leq H_1+X_1\\ H_3\leq x_3\leq H_3+X_3\\ x_1y\equiv x_3z \mod q}} 1. \end{aligned}$$

Considering the innermost summation, we have

$$\sum_{|y|\in\mathcal{K}(k)} \sum_{|z|\in\mathcal{J}(j)} \sum_{\substack{H_1\leq x_1\leq H_1+X_1\\ H_3\leq x_3\leq H_3+X_3\\ x_1y\equiv x_3z \mod q}} 1 \leq \sum_{1\leq|y|\leq e^kq/X_2} \sum_{1\leq|z|\leq e^jq/X_4} \sum_{\substack{H_1\leq x_1\leq H_1+X_1\\ H_3\leq x_3\leq H_3+X_3\\ x_1y\equiv x_3z \mod q}} 1.$$

Lemma 5.5 and the assumption

$$X_1 = X_4 \quad \text{and} \quad X_2 = X_3,$$

give

$$\begin{aligned} \sum_{|y|\in\mathcal{K}(k)} \sum_{|z|\in\mathcal{J}(j)} \sum_{\substack{H_1\leq x_1\leq H_1+X_1\\ H_3\leq x_3\leq H_3+X_3\\ x_1y\equiv x_3z \mod q}} 1 &\ll \frac{e^{k+j}qX_1X_3}{X_2X_4} \\ &\quad + \left(q + \frac{qe^kX_3}{X_2}\log q\right)^{1/2}\left(q + \frac{qe^kX_1}{X_4}\log q\right)^{1/2} \\ &\ll q\left(e^{k+j} + e^{(k+j)/2}\log q\right). \end{aligned}$$

This implies that

$$\begin{aligned} W &\ll qX_2X_4 \sum_{\substack{1\leq k\ll \log X_2\\ 1\leq j\ll \log X_4}} \min\left(U, \frac{X_4}{e^j}\right)\min\left(V, \frac{X_2}{e^k}\right)\left(1 + \frac{1}{e^{(k+j)/2}}\log q\right) \\ &= qX_2X_4\left(W_1 + W_2\log q\right), \end{aligned} \tag{5.11}$$

where

$$W_1 = \sum_{1\leq k\ll \log X_2} \min\left(V, \frac{X_2}{e^k}\right) \sum_{1\leq j\ll \log X_4} \min\left(U, \frac{X_4}{e^j}\right),$$

and

$$W_2 = \sum_{1\leq k\ll \log X_2} \frac{1}{e^{k/2}}\min\left(V, \frac{X_2}{e^k}\right) \sum_{1\leq j\ll \log X_4} \frac{1}{e^{j/2}}\min\left(U, \frac{X_4}{e^j}\right).$$

Considering W_1, we have

$$\begin{aligned}\sum_{1\le j\ll \log X_4} \min\left(U, \frac{X_4}{e^j}\right) &= \sum_{1\le j\le \log(X_4/U)+1} \min\left(U, \frac{X_4}{e^j}\right) \\ &\quad + \sum_{\log(X_4/U)+1\le j\ll \log X_4} \min\left(U, \frac{X_4}{e^j}\right) \\ &\ll U\log(X_4/U).\end{aligned}$$

In a similar fashion

$$\sum_{1\le k\ll \log X_2} \min\left(V, \frac{X_2}{e^k}\right) \ll V\log(X_2/V),$$

so that

$$W_1 \ll UV\log(X_4/U)\log(X_2/V).$$

Considering W_2, we have

$$\sum_{1\le j\ll \log X_4} \frac{1}{e^{j/2}} \min\left(U, \frac{X_4}{e^j}\right) \ll U \sum_{1\le j\ll \log X_4} \frac{1}{e^{j/2}} \ll U,$$

and

$$\sum_{1\le k\ll \log X_2} \frac{1}{e^{k/2}} \min\left(V, \frac{X_2}{e^k}\right) \ll V,$$

so that

$$W_2 \ll UV.$$

Inserting the above estimates into (5.11) gives

$$W \ll qX_2X_4UV\left(\log(X_4/U)\log(X_2/V) + \log q\right).$$

This implies that

$$\begin{aligned}J_2(X,H,V,U) &= \frac{X_1X_2X_3X_4UV}{q} \\ &\quad + O\left(UVX_2X_4\left(\log(X_4/U)\log(X_2/V) + \log q\right)\right).\end{aligned}$$

□

Our next step is to remove the conditions (5.7) and (5.8) in Lemma 5.6.

Corollary 5.7. *For any X, H, U, V with $V < X_2/2$ we have*

$$\begin{aligned}J_1(X,H,V) &= \frac{X_1X_2X_3X_4V}{q} \\ &\quad + O\left(V(X_1X_2X_3X_4)^{1/2}\log q\left(\log(X_2/V) + \log^{1/2} q\right)\right),\end{aligned}$$

and

$$J_2(X,H,V,U) = \frac{UVX_1X_2X_3X_4}{q} + O\left(UV(X_1X_2X_3X_4)^{1/2}\left(\log q + \log^2(X_2/V)\right)^{1/2}\left(\log q + \log^2(X_4/U)\right)^{1/2}\right).$$

Proof. We have

$$\begin{aligned} J_1(X,H,V) &= \frac{1}{q-1}\sum_{\substack{H_i\le x_i\le H_i+X_i\\ 1\le v\le V}}\sum_{\chi}\chi\left(x_1(x_2+v)x_3^{-1}x_4^{-1}\right) \\ &= \frac{X_1X_2X_3X_4V}{q-1} + \frac{1}{q-1}\sum_{\substack{H_i\le x_i\le H_i+X_i\\ 1\le v\le V}}\sum_{\substack{\chi\\ \chi\neq\chi_0}}\chi\left(x_1(x_2+v)x_3^{-1}x_4^{-1}\right). \end{aligned}$$

Let

$$W = \sum_{\substack{H_i\le x_i\le H_i+X_i\\ 1\le v\le V}}\sum_{\substack{\chi\\ \chi\neq\chi_0}}\chi\left(x_1(x_2+v)x_3^{-1}x_4^{-1}\right),$$

so that

$$W \le \sum_{\substack{\chi\\ \chi\neq\chi_0}}\left|\sum_{\substack{H_i\le x_i\le H_i+X_i\\ 1\le v\le V}}\chi((x_2+v)x_3^{-1})\right|\left|\sum_{H_i\le x_i\le H_i+X_i}\chi(x_1x_4^{-1})\right|.$$

An application of the Cauchy-Schwarz inequality gives

$$W^2 \le \left(\sum_{\substack{\chi\\ \chi\neq\chi_0}}\left|\sum_{\substack{H_i\le x_i\le H_i+X_i\\ 1\le v\le V}}\chi((x_2+v)x_3^{-1})\right|^2\right)\left(\sum_{\substack{\chi\\ \chi\neq\chi_0}}\left|\sum_{H_i\le x_i\le H_i+X_i}\chi(x_1x_4^{-1})\right|^2\right).$$

By Lemma 5.4 we have

$$\sum_{\substack{\chi\\ \chi\neq\chi_0}}\left|\sum_{H_i\le x_i\le H_i+X_i}\chi(x_1x_4^{-1})\right|^2 \ll qX_1X_4\log^2 q,$$

and by Lemma 5.6

$$\sum_{\substack{\chi\\ \chi\neq\chi_0}}\left|\sum_{\substack{H_i\le x_i\le H_i+X_i\\ 1\le v\le V}}\chi((x_2+v)x_3^{-1})\right|^2 \ll qX_2X_3V^2\left(\log(X_2/V)^2+\log q\right).$$

This implies that

$$W \ll qV(X_1X_2X_3X_4)^{1/2}\log q\left(\log(X_2/V)+\log^{1/2}q\right),$$

and hence

$$\begin{aligned}J_1(X,H,V) &= \frac{X_1X_2X_3X_4V}{q-1}\\ &\quad + O\left(V(X_1X_2X_3X_4)^{1/2}\log q\left(\log(X_2/V)+\log^{1/2}q\right)\right).\end{aligned}$$

The result follows since we have the bound

$$\frac{VX_1X_2X_3X_4}{q-1}-\frac{VX_1X_2X_3X_4}{q}\ll V(X_1X_2X_3X_4)^{1/2},$$

whenever

$$X_1X_2X_3X_4\ll q^4,$$

which we may assume.

Considering $J_2(X,H,V,U)$, let W be defined by

$$\left|J_2(X,H,V,U)-\frac{UVX_1X_2X_3X_4}{q-1}\right|=\frac{1}{q-1}W,$$

so that

$$W\le\sum_{\substack{\chi\\ \chi\neq\chi_0}}\left|\sum_{\substack{H_i\le x_i\le H_i+X_i\\ 1\le v\le V}}\chi((x_2+v)x_3^{-1})\right|\left|\sum_{\substack{H_i\le x_i\le H_i+X_i\\ 1\le u\le U}}\chi((x_4+u)x_1^{-1})\right|.$$

An application of the Cauchy-Schwarz inequality and Lemma 5.6 give

$$W\ll qUV(X_1X_2X_3X_4)^{1/2}\left(\log q+\log^2(X_2/V)\right)^{1/2}\left(\log q+\log^2(X_4/U)\right)^{1/2}.$$

Hence

$$\begin{aligned}J_2(X,H,V,U) &= \frac{UVX_1X_2X_3X_4}{q-1}\\ &+O\left(UV(X_1X_2X_3X_4)^{1/2}\left(\log q+\log^2(X_2/V)\right)^{1/2}\left(\log q+\log^2(X_4/U)\right)^{1/2}\right).\end{aligned}$$

□

We next improve on the error in J_1 by relating it to an average over J_2.

Lemma 5.8. *For any X, H and $V \leq X_2/2$ we have*

$$J_1(X,H,V) = \frac{VX_1X_2X_3X_4}{q} + O\left(V(X_1X_2X_3X_4)^{1/2}\log^{1/2} q\left(\log q + \log^2\left(X_2/V\right)\right)^{1/2}\right).$$

Proof. Let $J_1'(x_4)$ denote the number of solutions to the congruence

$$x_1(x_2+v) \equiv x_3x_4 \mod q,$$

in variables x_1, x_2, x_3 and v satisfying

$$H_i \leq x_i \leq H_i + X_i, \quad 1 \leq v \leq V,$$

so that

$$J_1(X,H,V) = \sum_{H_4 \leq x_4 \leq H_4+X_4} J_1'(x_4). \tag{5.12}$$

Let

$$U = \left\lfloor \frac{\log\log q}{\log^2 q} X_4 \right\rfloor.$$

For any integer $1 \leq u \leq U$ we have by (5.12)

$$\begin{aligned} J_1(X,H,V) &= \sum_{H_4-u \leq x_4 \leq H_4+X_4-u} J_1'(x_4+u) \\ &= \sum_{H_4 \leq x_4 \leq H_4+X_4} J_1'(x_4+u) \\ &\quad + \sum_{H_4-u \leq x_4 < H_4} J_1'(x_4) - \sum_{H_4+X_4-u \leq x_4 \leq H_4+X_4} J_1'(x_4). \end{aligned}$$

The term

$$\sum_{H_4-u \leq x_4 < H_4} J_1'(x_4),$$

is equal to the number of solutions to the congruence

$$x_1(x_2+v) \equiv x_3x_4 \mod q,$$

in variables x_1, x_2, x_3, x_4, v satisfying

$$H_i \leq x_i \leq H_i + X_i, \quad i = 1,2,3, \quad H_4 - u \leq x_4 < H_4, \quad 1 \leq v \leq V.$$

By an application of Corollary 5.7 we get

$$\sum_{H_4-u\le x_4<H_4} J_1'(x_4) = \frac{X_1X_2X_3Vu}{q} + O\left(V(X_1X_2X_3U)^{1/2}\log q\left(\log\left(X_2/V\right)+\log^{1/2} q\right)\right),$$

and

$$\sum_{H_4+X_4-u\le x_4\le H_4+X_4} J_1'(x_4) = \frac{X_1X_2X_3Vu}{q} + O\left(V(X_1X_2X_3U)^{1/2}\log q\left(\log\left(X_2/V\right)+\log^{1/2} q\right)\right).$$

This implies that

$$\begin{aligned} J_1(X,H,V) &= \sum_{H_4\le x_4\le H_4+X_4} J_1'(x_4+u) \\ &\quad + O\left(V(X_1X_2X_3U)^{1/2}\log q\left(\log\left(X_2/V\right)+\log^{1/2} q\right)\right) \\ &= \frac{1}{U}\sum_{1\le u\le U}\sum_{H_4\le x_4\le H_4+X_4} J_1'(x_4+u) \\ &\quad + O\left(V(X_1X_2X_3U)^{1/2}\log q\left(\log\left(X_2/V\right)+\log^{1/2} q\right)\right). \end{aligned}$$

The term

$$\sum_{1\le u\le U}\sum_{H_4\le x_4\le H_4+X_4} J_1'(x_4+u),$$

is equal to the number of solutions to the congruence

$$x_1(x_2+v)\equiv x_3(x_4+u) \mod q,$$

in variables x_1, x_2, x_3, x_4, v, u satisfying

$$H_i\le x_i\le H_i+X_i,\quad 1\le v\le V,\quad 1\le u\le U,$$

so that Corollary 5.7 and the assumption $V\le X_2/2$ give

$$\sum_{1\le u\le U}\sum_{H_4\le x_4\le H_4+X_4} J_1'(x_4+u) = \frac{UVX_1X_2X_3X_4}{q} + O\left(UV(X_1X_2X_3X_4)^{1/2}\left(\log q+\log^2\left(X_2/V\right)\right)^{1/2}\left(\log q+\log^2\left(X_4/U\right)\right)^{1/2}\right).$$

This implies that

$$\begin{aligned} J_1(X,H,V) &= \frac{VX_1X_2X_3X_4}{q} \\ &\quad + O\left(V(X_1X_2X_3U)^{1/2}\log q\left(\log\left(X_2/V\right)+\log^{1/2}q\right)\right) \\ &\quad + O\left(V(X_1X_2X_3X_4)^{1/2}\left(\log q+\log^2\left(X_2/V\right)\right)^{1/2}\left(\log q+\log^2\left(X_4/U\right)\right)^{1/2}\right). \end{aligned}$$

Recalling the choice of U we get

$$\begin{aligned} J_1(X,H,V) &= \frac{VX_1X_2X_3X_4}{q} \\ &\quad + O\left(V(X_1X_2X_3X_4)^{1/2}\log^{1/2}q\left(\log q+\log^2\left(X_2/V\right)\right)^{1/2}\right). \end{aligned}$$

□

5.6 Proof of Theorem 5.1

Let each $\mathcal{I}_i$ be defined by

$$\mathcal{I}_i = [H_i, H_i + X_i],$$

so we may write

$$N(\mathcal{I}) = J(X,H). \tag{5.13}$$

Let $J'(x_2)$ denote the number of solutions to the congruence

$$x_1x_2 \equiv x_3x_4 \mod q,$$

in variables x_1, x_3, x_4 satisfying

$$H_i \le x_i \le H_i + X_i,$$

so that

$$J(X,H) = \sum_{H_2 \le x_2 \le H_2+X_2} J_1'(x_2).$$

Let V be defined by

$$V = \left\lfloor \frac{X_2}{\log^2 q} \right\rfloor.$$

For any integer $1 \le v \le V$ we have

$$\begin{aligned} J(X,H) &= \sum_{H_2 \le x_2 \le H_2+X_2} J_1'(x_2+v) \\ &\quad + \sum_{H_2 - v \le x_2 < H_2} J_1'(x_2) - \sum_{H_2+X_2-v \le x_2 \le H_2+X_2} J_1'(x_2). \end{aligned}$$

The term

$$\sum_{H_2-v\le x_2<H_2} J_1'(x_2),$$

is equal to the number of solutions to the congruence

$$x_1x_2 \equiv x_3x_3 \mod q,$$

with variables satisfying

$$H_2 \le x_2 \le H_2+v, \quad H_i \le x_i \le H_i+X_i, \quad i=1,3,4.$$

An application of Lemma 5.4 gives

$$\sum_{H_2-v\le x_2<H_2} J_1'(x_2) = \frac{vX_1X_3X_4}{q} + O\left((VX_1X_3X_4)^{1/2}\log^2 q\right).$$

A similar argument gives

$$\sum_{H_2+X_2-v\le x_2\le H_2+X_2} J'(x_2) = \frac{vX_1X_3X_4}{q} + O\left((VX_1X_3X_4)^{1/2}\log^2 q\right),$$

so that

$$J(X,H) = \sum_{H_2\le x_2\le H_2+X_2} J'(x_2+v) + O\left((VX_1X_3X_4)^{1/2}\log^2 q\right).$$

Averaging over $1 \le v \le V$ we get

$$\begin{aligned} J(X,H) &= \frac{1}{V}\sum_{1\le v\le V}\sum_{H_2\le x_2\le H_2+X_2} J'(x_2+v) + O\left((VX_1X_3X_4)^{1/2}\log^2 q\right) \\ &= \frac{1}{V}J_1(X,H,V) + O\left((VX_1X_3X_4)^{1/2}\log^2 q\right). \end{aligned} \tag{5.14}$$

By Lemma 5.8 we have

$$\frac{1}{V}J_1(X,H,V) = \frac{X_1X_2X_3X_4}{q} + O\left((X_1X_2X_3X_4)^{1/2}\log^{1/2} q\left(\log q + \log^2(X_2/V)\right)^{1/2}\right),$$

so that substituting the above into (5.14) gives

$$\begin{aligned} J(X,H) = \frac{X_1X_2X_3X_4}{q} &+ O\left((X_1X_2X_3X_4)^{1/2}\log^{1/2} q\left(\log q + \log^2(X_2/V)\right)^{1/2}\right) \\ &+ O\left((VX_1X_3X_4)^{1/2}\log^2 q\right), \end{aligned}$$

and the result follows by (5.13) and recalling the choice of V.

Bibliography

[1] A. Ayyad, T. Cochrane and Z. Zheng, *The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$, and Mean Values of Character Sums*, J. Number Theory, **59**, 398–413, (1996).

[2] W. D. Banks, G. Harman and I. E. Shparlinski, *Distributional properties of the largest prime factor*, Michigan Math. J., **53** (2005), 665–681.

[3] W. D. Banks and I. E. Shparlinski, *Congruences and rational exponential sums with the Euler function*, Rocky Mountain J. Math., **36** (2006), 1415–1426.

[4] J. Bourgain, *Exponential sum estimates on subgroups of $\mathbb{Z}_q$, q arbitrary*, J. Anal. Math., **97** (2005), 317–355.

[5] J. Bourgain, *Fourier transform restriction phenomena for certain lattice subsets and applications to nonlinear evolution equations, Part I: Schrödinger equations*, Geom. Funct. Anal. **3**, 209–262, (1993), no. 3.

[6] J. Bourgain and M. C. Chang, *On a multilinear character sum of Burgess*, C. R. Acad. Sci. Paris, Ser. I **348** (2010), 115–120.

[7] J. Bourgain and C. Demeter, *Decouplings for curves and hypersurfaces with nonzero Gaussian curvature*, J. d'Analyse Math. (to appear), (2014), arXiv:1409.1634.

[8] J. Bourgain, C. Demeter and L. Guth, *Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three*, Ann. Math. (to appear).

[9] D. A. Burgess, *On character sums and L-series, I*, Proc. London Math. Soc. **12**, 1962, 193–206.

[10] D. A. Burgess, *On character sums and L-series, II*, Proc. London Math. Soc. **13**, 1963, 524–536.

[11] D. A. Burgess *A note on character sums for binary quadratic forms*, J. London Math. Soc. **43**, 1968, 271–274.

[12] D. A. Burgess, *Mean values of character sums*, Mathematika, **33**, no.1, 1–5, (1986).

[13] D. A. Burgess, *The character sum estimate with $r = 3$*, J. London Math. Soc. **33** (1986), 219–226.

[14] F. Chamizo, *On twisted character sums*, Archiv. Math., **96**, 2001, 417–421.

[15] M. C. Chang, *An Estimate of Incomplete Mixed Character Sums*, Bolyai Society Mathematical Studies, **21**, 2010, 243–250.

[16] J. Cilleruelo, *Combinatorial problems in finite fields and Sidon sets*, Combinatorica, **32**, no. 5, 497–511, (2012).

[17] J. Cilleruelo and A. Zumalacarregui, *Saving the logarithmic factor in the error term estimates of some congruence problems*, A. Math. Z. (2016). doi:10.1007/s00209-016-1771-1.

[18] T. Cochrane and S. Sih, *The congruence $x_1x_2 \equiv x_3x_4$ (mod m) and mean values of character sums*, J. Number Theory, **130**, 767–785, (2010).

[19] E. Cohen, *Arithmetical notes, V. A divisibility property of the divisor function*, Amer. Jour. Math., **83**, (1961), 693–697.

[20] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Springer-Verlag (New York), 2000.

[21] J. M. Deshouillers and H. Iwaniec, *An additive divisor problem*, J. London Math. Soc., **26**, (1982), 1–14.

[22] P. Enflo, *Some problems in the interface between number theory, harmonic analysis and geometry of Euclidian space, First International Conference in Abstract Algebra*, Quaestiones Math. **18**, (1995), no. 1-3, 309–323.

[23] V. Ennola, *On numbers with small prime divisors*, Ann. Acad. Sci. Fenn. Ser. Al, **440**, 1–16 (1969).

[24] P. Erdős and L. Mirsky, *The distribution of values of the divisor function $d(n)$*, Proc. London Math. Soc., **2**, (1952), 257–271.

[25] E. Fouvry, E. Kowalski and P. Michel, *Algebraic trace functions over the primes*, Duke Math. J. **9** (2014), 1683–1736.

[26] J. B. Friedlander, K. Gong and I. E. Shparlinski, *Character sums over shifted primes*, Mat. Zametki **88** (2010), 605–619.

[27] J.B. Friedlander, H. Iwaniec, *The divisor problem for arithmetic progressions*, Acta Arith. **45**, 273–277, (1985).

[28] J. B. Friedlander and H. Iwaniec, *Estimates for character sums*, Proc. Amer. Math. Soc. **119**, no. 2, 365–372, (1993).

[29] M. Z. Garaev, *On the logarithmic factor in error term estimates in certain additive congruence problems*, Acta. Arith. **124**, 27–39, (2006).

[30] M. Z. Garaev, *An estimate of Kloosterman sums with prime numbers and an application*, Mat. Zametki **88** , 365–373, (2010).

[31] M. Z. Garaev and V.C. Garcia, *The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications*, J. Number Theory, **128**, 2520–2537, (2008).

[32] A. Granville, *The lattice points of an n-dimensional tetrahedron*, Aequationes Math., **41**, 234–241, (1991).

[33] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[34] G. Harman, *Diophantine approximation with square-free integers*, Math. Proc. Cambridge Philos. Soc. **95**, 381–388, (1984).

[35] D. R. Heath-Brown, *Hybrid bounds for Dirichlet L-functions*, Invent Math. **47**, 149–170 (1978).

[36] D. R. Heath-Brown, *The divisor function at consecutive integers*, Mathematika, **31**, 141–149, (1984).

[37] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from k-th powers, and for Heilbronns exponential sum*, *Quart. J. Math.*, **51**, 221–235, (2000).

[38] D. R. Heath-Brown and L. B. Pierce, *Burgess bounds for short mixed character sums*, J. London Math. Soc. (2) **91**, no 2, 693–708, (2015).

[39] K. Henriot and K. Hughes, *Discrete restriction estimates of epsilon-removal type for kth-powers and k-paraboloids*, arXiv:1610.03984.

[40] A. Hilderbrand and G. Tenenbaum, *On integers free of large prime factors*, Trans. Amer. Math. Soc. **296**, 265–290, (1986).

[41] C. Hooley, *On Waring's problem for two squares and three cubes*, J. Reine Angew. Math. **328**, 161–207, (1981).

[42] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Colloq. Publ. **53**, Amer. Math. Soc. (Providence), 2004.

[43] A. A. Karatsuba, *Sums of characters over prime numbers*, Math. USSR Izv. **4**, 303–326, (1970).

[44] S. V. Konyagin, *Estimates of Character Sums in Finite fields*, Math. Notes, Vol. 88, No. 4, 503–515, (2010).

[45] N. M. Korobov, *On the distribution of digits in periodic fractions*, Matem. Sbornik, **89**, 654–670, (1972).

[46] D. H. Lehmer, *The lattice points of an n-dimensional tetrahedron*, Duke J. Math. **7**, 341–353, (1940).

[47] F. Luca and I. E. Shparlinski, *On the values of the divisor function*, Monatsh. Math. **154**, 59-69, (2008).

[48] H. L. Montgomery and R.C. Vaughan, *Mean values of character sums*, Canad. J. Math. **31**, no. 3, 476–487, (1979).

[49] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory I. Classical Theory*, Cambridge University Press, 2007.

[50] K. K. Norton, *Numbers with small prime factors and the least kth power non residue*, Mem. Amer. Math. Soc., **106**, Amer. Math. Soc., Providence, PI, (1971).

[51] W. Narkiewicz, *Uniform Distribution of Sequences of Integers in Residue Classes*, Springer-Verlag, 1984.

[52] S. Parsell, S. M. Prendiville, and T. D. Wooley, *Near-optimal mean value estimates for mul tidimensional Weyl sums*, Geom. Funct. Anal. **23**, no. 6, 1962–2024, (2013).

[53] L.B. Pierce, *Burgess bounds for multi-dimensional short mixed character sums*, J. Number Theory, **163**, 172–210, (2016).

[54] Z. Kh. Rakhmonov, *Estimation of the sum of characters with primes*, Dokl. Akad. Nauk Tadzhik. SSR **29**, 16–20, (1986).

[55] Z. Kh. Rakhmonov, *On the distribution of values of Dirichlet characters and their applications*, Proc. Steklov Inst. Math. **207**, 263–272, (1995).

[56] Z. Kh. Rakhmonov, *Sums of characters over prime numbers*, Chebyshevskii Sb, **15**, 73–100, (2014).

[57] R. A. Rankin, *The difference between consecutive prime numbers*, J. London Math. Soc. **36**, 242–247, (1938).

[58] L. G. Sathe, *On a Congruence Property of the Divisor Function*, Am. Jour. Math., **67**, 397–406, (1945).

[59] W. Schmidt. *Euqations over finite fields. An elementary approach.* Lecture notes in Math. **536**, Springer Verlag, 1976.

[60] R. C. Vaughan, *An elementary method in prime number theory*, Acta Arith. **37**, 111–115, (1980).

[61] A. Selberg, *Note on a paper by L.G. Sathe*, J. Indian Math. Soc., **18**, 83–87, (1954).

[62] I. D. Shkredov, *Some new inequalities in additive combinatorics*, MJCNT, **3**:2, 237–288, (2013).

[63] I. D. Shkredov, *On exponential sums over multiplicative subgroups of medium size*, Finite Fields Appl. **30**, 72–87, (2014).

[64] I. E. Shparlinski, 'Open problems on exponential and character sums', *Number Theory: Proc. 5th China-Japan Seminar, Osaka, 2008*, World Scientific, 222–242, (2010).

[65] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press, (1995).

[66] R.C. Vaughan, *Diophantine approximation by prime numbers, III*, Proc. London Math. Soc. **33**, 177–192, (1976).

[67] T. D. Wooley, *Approximating the Main Conjecture in Vinogradov's Mean Value Theorem*, 52. pp. arXiv:1401.2932, (2014).

[68] T. D. Wooley, *The cubic case of the Main Conjecture in Vinogradov's Mean Value Theorem*, Adv. Math. **294**, 532–561, (2016).

[69] T. D. Wooley, *Discrete Fourier restriction via efficient congruencing*, Internat. Math. Res. Notices, 48 pp. http://dx.doi.org/10.1093/imrn/rnw031.