SOME PROBLEMS ON EXPONENTIAL SUMS

NILANJAN BAG

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
GUWAHATI - 781039, INDIA

DECEMBER 2020

Some problems on exponential sums

by

Nilanjan Bag

(Roll No.: 156123024)

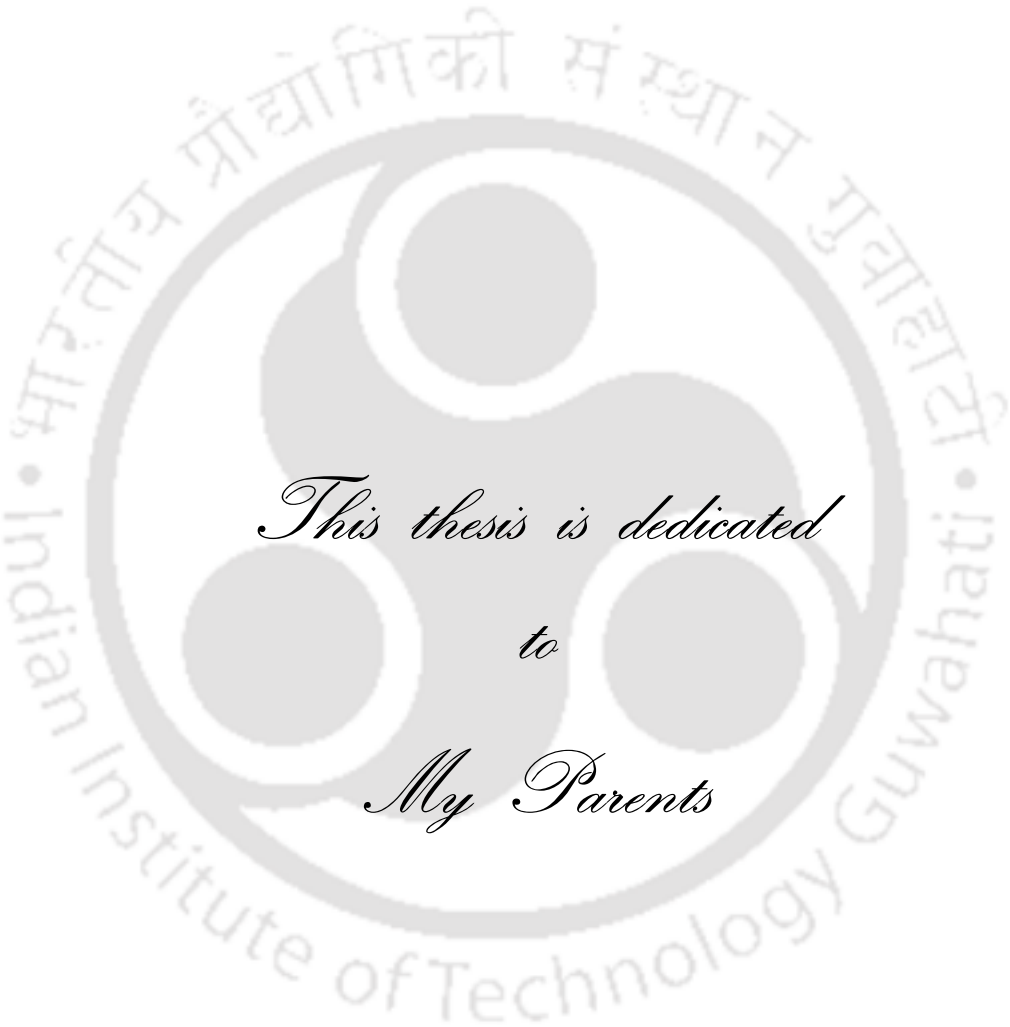
Department of Mathematics

submitted in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Guwahati
Guwahati - 781039, India

December 2020



This thesis is dedicated

to

My Parents

Certificate

This is to certify that the thesis entitled **Some problems on exponential sums** submitted by **Mr. Nilanjan Bag** to the **Indian Institute of Technology Guwahati**, for the award of the Degree of **Doctor of Philosophy**, is a record of the original bona fide research work carried out by him under my guidance and supervision. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Date: 24.12.2020
Guwahati, India

Dr. Rupam Barman
Associate Professor
Department of Mathematics
Indian Institute of Technology Guwahati

Acknowledgements

Words are indeed inadequate to convey my deep sense of gratitude to all those who helped me in completing this thesis work.

First and foremost, I am immensely grateful to my advisor Dr. Rupam Barman. I thank him for his guidance, encouragement and patience with me as a student during my research. He has been a strong motivation for me throughout this journey. This work would not have been possible without his endless support.

I thank the members of my doctoral committee, Prof. Anupam Saikia, Prof. K.V. Krishna, Dr. Vinay Wagh, for reviewing my research work periodically and for their constant support.

I would like to thank Prof. Igor E. Shparlinski for some fruitful discussions and insightful comments related to my work and for giving me the opportunity to collaborate with him. I express my sincere gratitude to Prof. Pierre Deligne for the proof of Lemma 3.4. I also thank Prof. Nicholas M. Katz, Prof. Todd Cochrane and Dr. Antonio Rojas-León for their valuable comments and suggestions during my PhD years.

I am grateful to all faculty members of the Department of Mathematics, IIT Guwahati for facilitating such a positive learning environment. I really enjoyed courses like Galois theory, algebraic number theory, modular forms, commutative algebra, lie algebra and many more offered by our department during my stay as

a student in the campus. I sincerely acknowledge IIT Guwahati for providing me various facilities necessary to carry out my research. I am also thankful to MHRD for providing the financial assistance for the completion of my thesis work.

Remembering some wonderful moments during my IIT Guwahati days, I thank all research scholars of our department for the encouragement.

My special thanks to my dear friend Reshmi, who has been a constant support and inspiration for me from the very first day I have started my journey as a research scholar. Also I would like to thank my dear friend Jaitra. All the mathematical and non-mathematical discussions with him definitely have a lasting effect in my mind.

Finally, I am grateful to my parents for their unconditional love and support which give me the strength to overcome all the difficult situations in life and boost my mind to achieve my goals.

Date: 24.12.2020

Guwahati, India Nilanjan Bag

Abstract

The central theme of this thesis is to study the moments of certain exponential sums, which we primarily capture by some asymptotic formulas. Our results are conceptual advancements to previously known methods and results on Kloosterman sums, generalized Gauss sums, and double exponential sums. Firstly, we introduce some new techniques to find the number of solutions of certain congruence equations modulo a prime p, which eventually allow us to obtain a sharper bound compared to previously known bounds for the fourth power mean of the 3-dimensional Kloosterman sum. We further employ our techniques to find an asymptotic formula for the fourth power mean of the 4-dimensional Kloosterman sum. Secondly, we study a conjecture of Wenpeng Zhang on higher order moments of the generalized quadratic Gauss sums weighted by L-functions. Previously known works on this conjecture used Weil's bound on curves, which seems to be insufficient to make further progress in proving the conjecture. We estimate some complicated character sums involving quadratic characters and find asymptotic formulas for such sums by relating these sums to traces of cohomology sheaves. With the help of the new estimates, we establish Zhang's conjecture upto weight 4. Thirdly, we study a problem on double exponential sums. The problem of estimating double exponential sums in prime fields is of a great interest in analytic number theory. We consider a double exponential sum where the range of the summation depends on some subsets $\mathcal{X}$ and $\mathcal{Y}$

of finite fields. As usually happens in this kind of sums, the problem is relatively easy when one or both subsets are initial intervals of the form $\{1, 2, ..., N\}$, for some integer N, as one can control the size of product of elements in the range. In our work we consider intervals of arbitrary position and propose a new approach which leads to a new estimate of the given sum.

Contents

Introduction

In this thesis, we mainly study four different problems on exponential and character sums. We study the asymptotic behaviour of certain exponential and character sums, namely *Kloosterman sums, quadratic Gauss sums,* and *double exponential sums*. The first part of the thesis is devoted to the study of Kloosterman sums.
Let q be any non-zero integer. For integers a and b, the classical *Kloosterman sum* is defined by

$$S(a,b;q) = \sum_{\substack{1\leq x\leq q\\(x,q)=1}} e\left(\frac{ax+b\overline{x}}{q}\right), \tag{1}$$

where $e(y) = e^{2\pi iy}$ and $\overline{x}$ denotes the multiplicative inverse of x mod q. In 1911, such an exponential sum first appeared in an article of Henri Poincaré [34] on the study of modular functions. In 1926, to study certain positive definite integral quadratic forms, H. D. Kloosterman [27] reintroduced this exponential sum. Later this sum was known as *Kloosterman sum*. H. D. Kloosterman had considerable interest in the order of magnitude of $S(a,b;q)$. He proved that

$$S(a,b;q) = O(q^{3/4+\epsilon}(a,q)^{1/4}) \qquad (q\to\infty), \tag{2}$$

for every positive ϵ. For primes $q = p$, the best possible bound till date is due to A. Weil. In paper [37], Weil proved that

$$|S(a, b; p)| \leq 2\sqrt{p}. \tag{3}$$

Kloosterman sums play quite an important role in modern analytic number theory, as well as the theory of automorphic forms, see for instance [20]. Indeed, H. D. Kloosterman showed in [26] that any non trivial upper bound for $S(a, b; q)$ gives a corresponding improvement of Hecke's upper bound for the Fourier coefficients of certain cusp forms. In view of such connections, mathematicians were interested in finding the order of magnitude of $S(a, b; q)$ and its arithmetic properties. One of the problems is to consider the moments of Kloosterman sums, namely

$$V_k(q) = \sum_{a \,(\mathrm{mod}\ q)} S^k(a, 1; q).$$

The original motivation to consider the moments directly follows from the work of H. D. Kloosterman, who wished to gain non-trivial bound for individual sums. This encouraged him to consider the problem in a global sense. It should be noted that N. M. Katz [22] has studied the higher moments from a modern point of view. From his result, one can deduce certain asymptotic formulas for any even power moments of $S(a, 1, q)$. In this thesis work, we mainly study asymptotic behaviour of mean values of certain higher-dimensional Kloosterman sums modulo a prime p.

The second part of the thesis is devoted to the study of quadratic Gauss sums. Let $q \geq 2$ be an integer, and let χ be a Dirichlet character modulo q. For $n \in \mathbb{Z}$, we define the *generalized quadratic Gauss sum* $G(n, \chi; q)$ as

$$G(n, \chi; q) = \sum_{a=1}^{q} \chi(a) e\left(\frac{na^2}{q}\right), \tag{4}$$

where $e(y) = e^{2\pi i y}$. This sum generalizes the classical *quadratic Gauss sum* $G(n; q)$,

which is defined as

$$G(n;q) = \sum_{a=1}^{q} e\left(\frac{na^2}{q}\right).$$

The properties of $G(n,\chi;q)$ have been studied for a long time. The values of $G(n,\chi;q)$ behave irregularly as χ varies. From a result of Cochrane and Zheng [11], we can deduce

$$|G(n,\chi;q)| \leq 2^{\omega(q)}\sqrt{q},$$

where $\omega(q)$ denotes the number of distinct prime divisors of q. In the case of prime q, finding such bounds is due to Gauss. For further study, also see [37].

The Dirichlet L-function $L(s,\chi)$ is defined by

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

where χ is a Dirichlet character modulo q and s is a complex variable with real part greater than 1. In analytic number theory, at times problems become very difficult to answer when specialised to L-functions. It has therefore been a common theme of research to study families of L-functions and this point of view has led to numerous insights. It has emerged from a series of results from last couple of decades that while studying L-functions on average, a remarkable array of results can be obtained if one has sufficiently strong information concerning the first and especially the second moment of the values of the L-functions on the critical line. More precisely, sometimes it is useful to study moments higher than the second moment, which are often captured by some asymptotic formulas, together with some basic information for individual L-functions. In this thesis work, we mainly study higher order moments of quadratic Gauss sums weighted by L-functions. We make progress in proving a conjecture of Wenpeng Zhang [40] on the product of quadratic Gauss sums and classical L-functions. Our approach towards the problem is a

conceptual advancement over earlier approaches to Zhang's conjecture.

The last part of the thesis is devoted to the study of double exponential sums. Let p be a prime. We denote the finite fields of p elements by $\mathbb{F}_p$ and denote the group of units of $\mathbb{F}_p$ by $\mathbb{F}_p^*$. Given sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_p$, we define the following sums

$$S_{a,r,s}(\mathcal{X}, \mathcal{Y}) = \sum_{x \in \mathcal{X}} \left| \sum_{y \in \mathcal{Y}} \mathbf{e}_p(ax^r y^s) \right|, \tag{5}$$

where

$$\mathbf{e}_p(z) = \exp(2\pi i z/p),$$

r and s are integers, and the powers in the exponent are computed in $\mathbb{F}_p$.

Clearly, in general settings without any restrictions on $\mathcal{X}$ and $\mathcal{Y}$ the presence of powers r and s in the definition of $S_{a,r,s}(\mathcal{X}, \mathcal{Y})$ is redundant, however they become important for some special sets $\mathcal{X}$ and $\mathcal{Y}$. In particular, these sums have been a very active object of study, especially when one or both sets are intervals of the form

$$\{A+1, \ldots, A+N\} \in [1, p-1] \tag{6}$$

of N consecutive residues modulo p. For example, when both $\mathcal{X}$ and $\mathcal{Y}$ are intervals, for bounds on such sums, with $(r, s) = (-1, -1)$, in which case they are called *incomplete double Kloosterman sums*, see [6, 8, 7, 17] and for the case $(r, s) = (1, -2)$, see [19]. The interest in such sums is instigated by the wealth of arithmetic applications. For example,

- Bourgain and Garaev [8, 7] have used bounds on such sums to obtain stronger versions of the *Brun–Titchmarsh theorem* on primes in arithmetic progressions;
- Friedlander and Iwaniec [17] have used these sums to derive new results on the divisor function in arithmetic progressions;

- Heath-Brown [19] has estimated such sums and applied them as a tool in deriving new bounds on the smallest square-free number in an arithmetic progression.

Organization of the Thesis

We present the entire work of this thesis in five chapters as described below.

- Chapter 1: Preliminaries
- Chapter 2: Fourth power mean of the 3-dimensional Kloosterman sums mod p
- Chapter 3: Fourth power mean of the 4-dimensional Kloosterman sums mod p
- Chapter 4: Higher order moments of generalized quadratic Gauss sums weighted by L-functions
- Chapter 5: Bounds on some double exponential sums

In Chapter 1, we define trace function and show how trace functions are related to cohomology sheaves. In this chapter, we briefly give few examples of trace functions, which will be used in subsequent chapters. We relate trace functions of more than one sheaf by describing a notion called correlation sum of traces. Also we discuss about few invariants related to sheaves like Swan conductors, conductors etc. Lastly, we describe absolute irreducibility of a polynomial, which we will use in Chapter 2.

In Chapter 2, we study fourth power mean of a general 3-dimensional Kloosterman sum mod p. Recently, Zhang and Lv have found an asymptotic formula for fourth power mean of a general 3-dimensional Kloosterman sum mod p. In this chapter we prove an improvement of their asymptotic formula.

In Chapter 3, we study fourth power mean of a general 4-dimensional Kloosterman sum mod p. We prove an asymptotic formula for a fourth power mean of

a general 4-dimensional Kloosterman sum. We use a result of P. Deligne, which counts the number of $\mathbb{F}_p$-points on the surface

$$(x-1)(y-1)(z-1)(1-xyz) - uxyz = 0, \ u \neq 0,$$

and then take an average of the error terms over u to prove the asymptotic formula. We also find the number of solutions of certain congruence equations mod p which we use to prove our main result.

In Chapter 4, we study higher order moments of the generalized quadratic Gauss sums weighted by L-functions using estimates for character sums and analytic methods. We find asymptotic formulas for three character sums which arise naturally in the study of higher order moments of the generalized quadratic Gauss sums. We then use these character sum estimates to find asymptotic formulas for the $6th$ and $8th$ order moments of the generalized quadratic Gauss sums weighted by L-functions.

In Chapter 5, we give a new bound of double sums with monomials over an interval and an arbitrary set in finite fields. This bound generalizes and in some cases improves previously known results.

1 Preliminaries

One of the most basic questions in number theory is to understand how various sets of integers behave when restricted to *congruence classes*. Given an integer $q \in \mathbb{Z} \setminus \{0\}$, a congruence class modulo q is a subset of the shape $a \pmod q = a + q\mathbb{Z} \subset \mathbb{Z}$, for some integer a.

In number theory, specially in analytic number theory one is interested in studying the behaviour of some given arithmetic functions along congruence classes, for instance to determine whether a set of integers has finite or infinite intersection with some congruence class. The analysis of such problem often involves certain specific classes of functions on $\mathbb{Z}/q\mathbb{Z}$. While studying such functions it is natural to apply

the *Chinese Remainder Theorem*, which is given as

$$\mathbb{Z}/q\mathbb{Z} \cong \prod_{p^\alpha \| q} \mathbb{Z}/p^\alpha\mathbb{Z},$$

where α is the highest power such that p^α divides q. It largely reduces the study to the case of prime power moduli. When the matter is as simple as possible, i.e., when q is a prime, then the ring $\mathbb{Z}/q\mathbb{Z}$ is a finite field $\mathbb{F}_q$ and often the functions that occur are what we call *trace functions*.

1.1 Characters

Trace functions modulo a prime p are special classes of $\mathbb{C}$-valued functions on $\mathbb{F}_p$. The most significant example, beyond the constant function 1, is the *Legendre symbol*, defined as

$$\left(\frac{\bullet}{p}\right) : x \in \mathbb{F}_p \to \begin{cases} 0 & \text{if } x = 0; \\ +1 & \text{if } x \in (\mathbb{F}_p^\times)^2; \\ -1 & \text{if } x \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2. \end{cases}$$

On the way to proving the famous theorem on primes in arithmetic progression, P. G. Dirichlet further enriched the class of trace functions. He introduced what we now call *Dirichlet characters*. These are homomorphism of multiplicative groups

$$\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times,$$

with $\chi(0) = 0$, for χ non-trivial. Another important example of trace functions are the additive characters, i.e., homomorphisms from additive group to multiplicative

group of complex numbers

$$\psi : (\mathbb{Z}/p\mathbb{Z}, +) \to \mathbb{C}^{\times}.$$

It is well know that, these all are of the shape

$$x(\in \mathbb{Z}/p\mathbb{Z}) \mapsto \mathbf{e}_p(ax),$$

where a is fixed in $\mathbb{Z}/p\mathbb{Z}$ and $\mathbf{e}_p(x) = e^{\frac{2\pi iax}{p}}$. Both additive and multiplicative characters satisfy the orthogonality relations

$$\sum_{x\in\mathbb{F}_p} \psi(x)\overline{\psi'(x)} = p\delta_{\psi\sim\psi'} \qquad \text{and} \qquad \sum_{x\in\mathbb{F}_p^{\times}} \chi(x)\overline{\chi'(x)} = (p-1)\delta_{\chi\sim\chi'},$$

where for two functions f and g, the delta function is defined by

$$\delta_{f\sim g} = \begin{cases} 1, & \text{if } f = g; \\ 0, & \text{if } f \neq g. \end{cases}$$

It is important to note that such orthogonality relations can be generalized to arbitrary trace functions.

1.2 Algebraic exponential sums

In 1926, while studying the case of a positive definite homogeneous polynomial of degree two in four variables and introducing a new variant of the circle method, H. D. Kloosterman defined the so called Kloosterman sum, which is defined in (1). This is another very important example of trace function, which is indeed defined via Fourier transformation. The bound (2) proved by H. D. Kloosterman plays a crucial role in the study of Diophantine equations. In 1948, this bound was improved

by André Weil [21, Section 11.7], who as a consequence of his work on the Riemann hypothesis for curves over finite fields proved the best individual upper bound as given in (3).

A further important example of trace function is *hyper-Kloosterman sums* denoted as $K(m, s; q)$ which were introduced by P. Deligne [13]. These are higher-dimensional generalisation of classical Kloosterman sums and defined as

$$K(m, s; q) = \sum_{x_1=1}^{q}{}' \cdots \sum_{x_s=1}^{q}{}' e\left(\frac{x_1 + \cdots + x_s + m\overline{x_1 \cdots x_s}}{q}\right) \tag{1.1}$$

for any fixed integer $s \geq 2$ and any positive integer $q \geq 3$. Here, $\sum_{x=1}^{q}{}'$ denotes the summation over all $1 \leq x \leq q$ such that $\gcd(x, q) = 1$, $e(y) = e^{2\pi i y}$, and $\overline{x}$ denotes the multiplicative inverse of x.

Hyper-Kloosterman sums can be interpreted as an inverse of Mellin transformation of powers of Gauss sums and therefore can be used to study the distribution of Gauss sums.

Now we are going to define some important terms and state some results, mostly following [15], which will be required to prove our main results.

1.3 Formal definition of trace functions

1.3.1 Galois representations

Let $\mathbb{P}^1_{\mathbb{F}_p}$ be the projective line and $\mathbb{A}^1_{\mathbb{F}_p} \subset \mathbb{P}^1_{\mathbb{F}_p}$ be the affine line and $K = \mathbb{F}_p(X)$ be the functions field over $\mathbb{F}_p$. Let $K^{sep} \supset K$ be the separable closure of K and $\overline{\mathbb{F}_p} \subset K^{sep}$ denote the algebraic closure of $\mathbb{F}_p$ in K^{sep}. We denote by G^{geom} and G^{arith} the *geometric* and *arithmetic* Galois group respectively, defined as

$$G^{geom} := \mathrm{Gal}\left(K^{sep}/\overline{\mathbb{F}_p} \cdot K\right) \subset G^{arith} := \mathrm{Gal}\left(K^{sep}/K\right).$$

By restricting the action of an element of G^{arith} to $\overline{\mathbb{F}_p}$, we have the exact sequence

$$1 \to G^{geom} \to G^{arith} \to \mathrm{Gal}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right) \to 1.$$

We denote by $\mathbb{P}^1_{\mathbb{F}_p}$, the set of closed points of degree 1 and $\mathbb{A}^1_{\mathbb{F}_p} = \mathbb{P}^1_{\mathbb{F}_p} \setminus \{\infty\}$. Note that $\mathbb{A}^1_{\mathbb{F}_p}$ is identified with $\mathbb{F}_p$ by identifying $x \in \mathbb{F}_p$ with the degree one polynomial $X - x$. A non-empty open set $U \subset \mathbb{A}^1_{\mathbb{F}_p}$ is the open complement of the closed set $Z_Q \subset \mathbb{A}^1_{\mathbb{F}_p}$ of the zeros of some polynomial Q and the set of closed points of degree one in U is identified with the complement of the set of roots of Q contained in $\mathbb{F}_p$:

$$U(\mathbb{F}_p) \simeq \{x \in \mathbb{F}_p : Q(x) \neq 0\}.$$

For $x \in \mathbb{P}^1_{\overline{\mathbb{F}_p}}$, consider the ring of rational functions defined in a neighbourhood of x and denote it by $\mathcal{O}_x$, whose field of fraction is K. Let $v_x : K \to \mathbb{Z} \cup \{\infty\}$ be the associated discrete valuation. We consider $\mathcal{O}_x = \{f \in K : v_x(f) \geq 0\}$ and $\mathfrak{p}_x = \{f \in K : v_x(f) > 0\}$, which is a maximal ideal. We denote by $k_x = \mathcal{O}_x/\mathfrak{p}_x$, its residue field and by p_x, the size of k_x, i.e., $p_x = p^{\deg\, x}$ where deg x is the degree over $\mathbb{F}_p$.

1.3.2 Decomposition group and inertia group

The valuation can be extended to a valuation on K^{sep}. We denote one such extension as $v_{\{x\}}$ which determines a decomposition group $D_{\{x\}}$ and an inertia group $I_{\{x\}}$ in the arithmetic Galois group, defined as

$$D_{\{x\}} = \{\sigma \in G^{arith} |\ v_{\{x\}} \circ \sigma = v_{\{x\}}\},$$

and

$$I_{\{x\}} = \{\sigma \in D_{\{x\}} |\ \sigma(x) \equiv x \pmod{\mathfrak{p}_{\{x\}}}, \forall x \in \mathcal{O}_{\{x\}}\}.$$

From the definitions of $D_{\{x\}}$ and $I_{\{x\}}$, we have

$$I_{\{x\}} \subset D_{\{x\}} \subset G^{arith}.$$

Also these groups satisfy the exact sequence

$$1 \to I_{\{x\}} \to D_{\{x\}} \to \mathrm{Gal}(\overline{\mathbb{F}_p}/k_x) \to 1.$$

Here $\mathrm{Gal}(\overline{\mathbb{F}_p}/k_x)$ is topologically generated by the *arithmetic Frobenius*

$$u \to u^{p_x}.$$

We denote the arithmetic Frobenius by $\mathrm{Frob}_{k_x}^{arith}$, which is defined over $\overline{\mathbb{F}_p}$. We call its inverse as the *geometric Frobenius* and denote it as $\mathrm{Frob}_{k_x}^{geom}$. The lifts of the geometric Frobenius defines an $I_{\{x\}}$ class in the decomposition group, which we denote by $\mathrm{Frob}_{\{x\}} \subset D_{\{x\}}$, and call as the Frobenius class at $\{x\}$.

Definition 1.1. *Given x, a closed point of $\mathbb{P}^1_{\mathbb{F}_p}$, a G^{arith}-module V is unramified (or lisse) at x if for any extension $\{x\}$, the corresponding inertia subgroup $I_{\{x\}}$ acts trivially on V. Otherwise V is ramified at x.*

If V is unramified at x, all the elements in the Frobenius class $\mathrm{Frob}_{\{x\}}$ acts by the same automorphism of V. We denote this automorphism by $(\mathrm{Frob}_{\{x\}}|V)$.

Fix some prime $\ell \neq p$, consider $\overline{\mathbb{Q}_\ell}$, the algebraic closure of the *ℓ-adic numbers* $\mathbb{Q}_\ell$. Trace functions modulo p are $\overline{\mathbb{Q}_\ell}$-valued functions defined on the set of $\mathbb{F}_p$-points of the affine line $\mathbb{A}^1_{\mathbb{F}_p}$. They are obtained from *ℓ-adic sheaves*, often denoted as $\mathcal{F}$.

Definition 1.2. *Let $U \subset \mathbb{A}^1_{\mathbb{F}_p}$ be a non-empty open subset of $\mathbb{A}^1_{\mathbb{F}_p}$ defined over $\mathbb{F}_p$. An ℓ-adic sheaf lisse on U, say $\mathcal{F}$, is a continuous finite-dimensional Galois representation*

$$\varrho_{\mathcal{F}} : G^{arith} \to GL(V_{\mathcal{F}}),$$

where $V_{\mathcal{F}}$ is a finite dimensional $\overline{\mathbb{Q}_\ell}$-vector space, which is unramified at every closed point x of U. Here the dimension of the vector space $V_{\mathcal{F}}$ is called the rank of $\mathcal{F}$ and is denoted by $\mathrm{rk}(\mathcal{F})$.

1.3.3 The trace function attached to a lisse sheaf

For $x \in U(\mathbb{F}_p)$, a closed point of degree one at which the representation $\varrho_{\mathcal{F}}$ is unramified, we have a Frobenius conjugacy class $(\mathrm{Frob}_x|V_{\mathcal{F}})$, namely the union of all the $(\mathrm{Frob}_{\{x\}}|V_{\mathcal{F}})$. By conjugacy the trace of all these automorphisms $(\mathrm{Frob}_{\{x\}}|V_{\mathcal{F}})$ is constant within that class. We denote this common value by $\mathrm{tr}(\mathrm{Frob}_x|V_{\mathcal{F}})$ and call it the Frobenius trace of $\mathcal{F}$ at x.

Definition 1.3. *Given an ℓ-adic sheaf $\mathcal{F}$ lisse on $U \subset \mathbb{A}^1_{\mathbb{F}_p}$, the trace function $K_{\mathcal{F}}$ is a function on $U(\mathbb{F}_p)$ given by*

$$x \in U(\mathbb{F}_p) \mapsto K_{\mathcal{F}}(x) = \mathrm{tr}(\mathrm{Frob}_x|V_{\mathcal{F}}).$$

These are $\overline{\mathbb{Q}_\ell}$-valued functions, but often can be considered as complex valued functions via the embedding

$$i : \overline{\mathbb{Q}_\ell} \to \mathbb{C}.$$

1.4 Representations types

The definition of sheaves and trace functions in terms of Galois representations enable to use the following terms from representation theory:

- An ℓ-adic sheaf is *irreducible* if the representation $\varrho_{\mathcal{F}}$ is *irreducible*.
- An ℓ-adic sheaf is *geometrically irreducible* if the restriction of $\varrho_{\mathcal{F}}$ to the geometric Galois group G^{geom} is *irreducible*.
- An ℓ-adic sheaf is *trivial* if the representation $\varrho_{\mathcal{F}}$ is *trivial*. In this case the trace function is constant 1.

One can also create new sheaves and trace functions from other sheaves. In the following we discuss about such constructions:

- Given two sheaves $\mathcal{F}$ and $\mathcal{G}$ lisse on U and U' respectively, one can form the direct sum sheaf $\mathcal{F} \oplus \mathcal{G}$ which is lisse on $U \cap U'$ and is of rank equal to the sum of the ranks of $\mathcal{F}$ and $\mathcal{G}$, and whose representation is $\varrho_{\mathcal{F}\oplus\mathcal{G}} = \varrho_{\mathcal{F}} \oplus \varrho_{\mathcal{G}}$. Its trace function is given by the sum

$$K_{\mathcal{F}\oplus\mathcal{G}}(x) = K_{\mathcal{F}}(x) + K_{\mathcal{G}}(x),$$

  for $x \in U(\mathbb{F}_p) \cap U'(\mathbb{F}_p)$.

- Similarly, one can form the tensor product sheaf $\mathcal{F} \otimes \mathcal{G}$ which is lisse on $U \cap U'$ with rank equal to the product of ranks of $\mathcal{F}$ and $\mathcal{G}$, whose representation is $\varrho_{\mathcal{F}\otimes\mathcal{G}} = \varrho_{\mathcal{F}} \otimes \varrho_{\mathcal{G}}$. The trace function for $\mathcal{F} \otimes \mathcal{G}$ is given by

$$K_{\mathcal{F}\otimes\mathcal{G}}(x) = K_{\mathcal{F}}(x)K_{\mathcal{G}}(x),$$

  for $x \in U(\mathbb{F}_p) \cap U'(\mathbb{F}_p)$.

- Let $f \in \mathbb{F}_p(X)$ be non-constant. We can view f as a non-constant morphism from $\mathbb{P}^1_{\mathbb{F}_p}$ to $\mathbb{P}^1_{\mathbb{F}_p}$. The Galois subgroup corresponding to this covering

$$\mathrm{Gal}(K^{sep}/\mathbb{F}_p(f(X))) \subset G^{arith}$$

is isomorphic to G^{arith} and therefore the restriction of $\varrho_{\mathcal{F}}$ to $\mathrm{Gal}(K^{sep}/\mathbb{F}_p(f(X)))$ defines an ℓ-adic sheaf on $\mathbb{P}^1_{\mathbb{F}_p}$ lisse on $f^{-1}(U)$ which is denoted as $f^*\mathcal{F}$ and is called the *pull-back* of $\mathcal{F}$ by f. Its rank is equal to the rank of $\mathcal{F}$ and its trace function is given by

$$K_{f^*\mathcal{F}}(x) = K_{\mathcal{F}}(f(x)),$$

for $x \in f^{-1}(U)(\mathbb{F}_p) \setminus \{\infty\}$. We will use this pull-back sheaf construction for the following morphisms. These are special cases of fractional linear transformations.

Given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_p)$, the group of automorphism of $\mathbb{P}^1_{\mathbb{F}_p}$, one defines the automorphism

$$[\gamma] : x \to \frac{ax+b}{cx+d}.$$

In particular, for

$$\gamma = n(b) = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix},$$

we obtain the additive translation map $x \mapsto x + b$ and for

$$\gamma = n(b) = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}, a \neq 0$$

we obtain the multiplicative translation map $x \mapsto ax$. We denote the pull-back sheaf by $\gamma^*\mathcal{F}$.

Next we discuss the size of trace functions.

Definition 1.4. *Let $w \in \mathbb{Z}$. An ℓ-adic sheaf $\mathcal{F}$ lisse on U is punctually pure of weight w, if for any $x \in U(\mathbb{F}_p)$, the eigenvalues of $(\mathrm{Frob}_x | V_{\mathcal{F}})$ are complex numbers of modulus $p_x^{w/2}$.*

A sheaf is mixed of weights $\leq w$ if as a representation it is a successive extension of sheaves punctually pure of weights $\leq w$.

If $\mathcal{F}$ is mixed of weights w, one has for any $x \in U(\mathbb{F}_p)$

$$|K_{\mathcal{F}}(x)| \leq \mathrm{rk}(\mathcal{F}) p^{w/2}.$$

It is always possible to reduce to the case of ℓ-adic sheaves mixed of weights $w \leq 0$. For any $w \in \mathbb{Z}$, there exists an ℓ-adic sheaf $\overline{\mathbb{Q}_\ell}(w/2)$ of rank 1, lisse on $\mathbb{P}^1_{\mathbb{F}_p}$, whose restriction to G^{geom} is trivial and $\overline{\mathbb{Q}_\ell}(w/2)$ is pure of weight $-w$. Given $\mathcal{F}$ of some weight w', the tensor product

$$\mathcal{F}(w/2) := \mathcal{F} \otimes \overline{\mathbb{Q}_\ell}(w/2)$$

has weight $w' - w$ and the trace function is given by

$$x \mapsto p^{-w/2} K_{\mathcal{F}}(x).$$

1.5 Local monodromy representations

Given an ℓ-adic sheaf $\mathcal{F}$, let $D_{\mathcal{F}}^{ram} \subset \mathbb{P}^1(\overline{\mathbb{F}_p}) \backslash U(\overline{\mathbb{F}_p})$ be the set of geometric points where $\varrho_{\mathcal{F}}$ is ramified, that is, the inertia group $I_{\{x\}}$ acts non-trivially. The restriction of the representations, $\varrho_{\mathcal{F}|I_{\{x\}}}$ is called the local monodromy representation of $\mathcal{F}$ at x.

This set of representations is fundamental to study $\mathcal{F}$ and its trace functions. Let $P_{\{x\}}$ be the p-Sylow subgroup of $I_{\{x\}}$. They sit in a standard short exact sequence

$$1 \to P_{\{x\}} \to I_{\{x\}} \to I_{\{x\}}^{tame} \to 1,$$

where $I_{\{x\}}^{tame}$ is the inertia quotient $I_{\{x\}}/P_{\{x\}}$. For details, see [23, Chapter 1].

Definition 1.5. *The sheaf $\mathcal{F}$ is called tamely ramified at x if $P_{\{x\}}$ acts trivially on $V_{\mathcal{F}}$ and is otherwise called wildly ramified.*

1.6 Some numerical invariants

If the representation is wildly ramified, then one can talk about a numerical invariant called the Swan conductor. There is a decreasing upper numeric filtration $I_{\{x\}}^{(\lambda)}$, indexed by real numbers $\lambda \geq 0$. Each $I_{\{x\}}^{(\lambda)}$ is normal in $D_{\{x\}}$, $I_{\{x\}}^{(0)} = I_{\{x\}}$ and $I_{\{x\}} \supset P_{\{x\}} \supset I_{\{x\}}^{(\lambda_1)} \supset I_{\{x\}}^{(\lambda_2)}$ for $0 < \lambda_1 < \lambda_2$. Furthermore,

$$P_{\{x\}} = \text{the closure of} \bigcup_{\lambda>0} I_{\{x\}}^{(\lambda)},$$

$$\{1\} = \bigcap_{\lambda>0} I_{\{x\}}^{(\lambda)} \text{ and } I_{\{x\}}^{(\lambda)} = \bigcap_{0<t<\lambda} I_{\{x\}}^{(t)}.$$

We can decompose $V_{\mathcal{F}}$ by a $P_{\{x\}}$-stable direct sum as

$$V_{\mathcal{F}} = \bigoplus_{\lambda \in \text{Break}(V_{\mathcal{F}})} V_{\mathcal{F}}(\lambda)$$

indexed by a finite set of rational numbers $\text{Break}(V_{\mathcal{F}}) \subset \mathbb{Q}$, the set of breaks of the $I_{\{x\}}$-module $V_{\mathcal{F}}$ such that

$$V_{\mathcal{F}}(0) = V_{\mathcal{F}}^{P_{\{x\}}};$$
$$V_{\mathcal{F}}(\lambda)^{I_{\{x\}}^{(\lambda)}} = 0, \ \forall \ \lambda > 0;$$

$$V_{\mathcal{F}}(\lambda)^{I_{\{x\}}^{(\lambda')}} = V_{\mathcal{F}}(\lambda),\ \forall\ \lambda' > \lambda.$$

For more details see [23, Chapter 1]. The *Swan conductor* is defined as

$$\mathrm{Swan}_x(\mathcal{F}) = \sum_{\lambda \in \mathrm{Break}(V)} \lambda\ \dim(V_{\mathcal{F}}(\lambda)).$$

Using [23, Prop. 1.9] one can show that the Swan conductor is always an integer. Now we define a numerical invariant which is a measure of complexity of a sheaf.

Definition 1.6. *We define the conductor of $\mathcal{F}$, denoted as $C(\mathcal{F})$, via the following formula*

$$C(\mathcal{F}) = \mathrm{rk}(\mathcal{F}) + |\mathbb{P}^1(\overline{\mathbb{F}_p}) - U(\overline{\mathbb{F}_p})| + \sum_{x \in D_{\mathcal{F}}^{ram}(\overline{\mathbb{F}_p})} \mathrm{Swan}_x(\mathcal{F}).$$

1.7 Some important cohomology sheaves

We now give few examples of cohomology sheaves which we will study or use as a tool in our work in the thesis.

1.7.1 Trivial sheaf

The trivial representation $\overline{\mathbb{Q}_\ell}$ is everywhere unramified with pure weight 0, rank 1 and the conductor 1. Its trace function is $K_{\overline{\mathbb{Q}_\ell}}(x) = 1$.

1.7.2 Kummer sheaf

For any non-trivial Dirichlet character $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$, there exists an ℓ-adic sheaf $\mathcal{L}_\chi$, called as Kummer sheaf, of rank 1 with pure weight 0, unramified on $\mathbb{P}^1_{\mathbb{F}_p} \setminus \{0, \infty\}$. Its trace function is $K_{\mathcal{L}_\chi}(x) = \chi(x)$ and conductor $C(\mathcal{L}_\chi) = 3$.

1.7.3 Legendre sheaf

It is a non-trivial cohomology sheaf, denoted as $\mathcal{F}$, associated to the Legendre family of elliptic curves over the t-line

$$y^2 = x(x-1)(x-t),$$

where $t \in \mathbb{F}_p$. It is of rank 2 with pure weight 1. The trace function associated to $\mathcal{F}$ is given by

$$K_{\mathcal{F}}(t) = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right)\left(\frac{x-1}{p}\right)\left(\frac{x-t}{p}\right),$$

where $\left(\frac{\bullet}{p}\right)$ is the Legendre symbol. For a more detailed study, see [24, Chapter 15].

1.7.4 Kloosterman sheaf

In [12], P. Deligne gave a proof of the last Weil conjecture (Riemann hypothesis) for algebraic varieties over finite fields and in [14] gave a generalisation to weights of ℓ-adic sheaves on such varieties. Another deep result is the construction of an ℓ-adic Fourier transform, corresponding to the discrete Fourier transform at the level of trace functions, with a control of the weights. In particular he constructed hyper-Kloosterman sums, which are defined in (1.1), as a trace functions of ℓ-adic sheaves. This sum was subsequently studied in depth by N. M. Katz in [23].

1.8 Quasi-orthogonality relations

Given two ℓ-adic sheaves $\mathcal{F}$ and $\mathcal{G}$ both lisse on some non-empty open set $U \subset \mathbb{A}^1_{\mathbb{F}_p}$ and both pure of weight 0, consider the tensor product $\mathcal{F} \otimes D(\mathcal{G})$, where $D(\mathcal{G})$ is the dual sheaf of $\mathcal{G}$. Here the dual-sheaf $D(\mathcal{G})$ is the contragredient representation $D(\varrho_{\mathcal{F}})$ on the dual space $\mathrm{Hom}(V_{\mathcal{F}}, \overline{\mathbb{Q}_l})$. The sheaf $\mathcal{F} \otimes D(\mathcal{G})$ is also lisse on U and

pure of weight 0. Moreover from the definition of conductors one sees that

$$C(\mathcal{F} \otimes D(\mathcal{G})) \leq C(\mathcal{F})C(\mathcal{G}).$$

The trace functions of $\mathcal{F} \otimes D(\mathcal{G})$ are given by

$$x \mapsto K_{\mathcal{F}\otimes D(\mathcal{G})}(x) = K_{\mathcal{F}}(x)\overline{K_{\mathcal{G}}(x)},$$

for $x \in U(\mathbb{F}_p)$. Therefore the trace formula can be used to evaluate the *correlation sums* between the trace functions of $\mathcal{F}$ and $\mathcal{G}$, defined as

$$C(\mathcal{F}, \mathcal{G}) := \frac{1}{p}\sum_{x\in\mathbb{F}_p} K_{\mathcal{F}}(x)\overline{K_{\mathcal{G}}(x)}.$$

1.8.1 Decomposition of sheaves and trace functions

P. Deligne, on his way to the proof of the Riemann Hypothesis for projective varieties over finite fields established that any ℓ-adic sheaf, pure of weight zero, is geometrically semi-simple, that is the representation $\varrho_{\mathcal{F}|G^{geom}}$ decomposes into a direct sum of irreducible representations of G^{geom}. The irreducible components occurring in the decomposition of $\varrho_{\mathcal{F}|G^{geom}}$ are called the *geometric irreducible components* of $\mathcal{F}$. Considering semi-simplification, one can get

$$\varrho_{\mathcal{F}} = \bigoplus_{i\in I} \varrho_{\mathcal{F}_i}$$

where $\varrho_{\mathcal{F}_i}$ are arithmetically irreducible and lisse on U. Since semi-simplification does not change the trace functions, one obtains a decomposition of trace function

$$K_{\mathcal{F}} = \sum_i K_{\mathcal{F}_i}.$$

Theorem 1.1. *[15, Theorem 5.2](Quasi-orthogonality relation) Suppose that $\mathcal{F}$ and*

$\mathcal{G}$ both are punctually pure of weight 0 and both are geometrically irreducible with $n_{\mathcal{F}}$ copies of the irreducible component $\overline{\mathcal{F}_{irr}}$ for $\mathcal{F}$ and $n_{\mathcal{G}}$ copies of the irreducible component $\overline{\mathcal{G}_{irr}}$ for $\mathcal{G}$. Then we have

$$\mathcal{C}(\mathcal{F},\mathcal{G}) = \left(\sum_{i=1}^{n_{\mathcal{F}}\cdot n_{\mathcal{G}}} \alpha_{i,\mathcal{F},\mathcal{G}}\right)\delta_{\overline{\mathcal{F}}\sim_{geom}\mathcal{G}} + O\left(\frac{C(\mathcal{F})^2C(\mathcal{G})^2}{p^{1/2}}\right),$$

where $\alpha_{i,\mathcal{F},\mathcal{G}}$ is a complex number of modulus 1. In particular, if $\mathcal{F}$ and $\mathcal{G}$ are both geometrically irreducible, then there exists $\alpha_{\mathcal{F},\mathcal{G}} \in S^1$ such that

$$C(\mathcal{F},\mathcal{G}) = \alpha_{\mathcal{F},\mathcal{G}}\delta_{\overline{F}\sim_{geom}\mathcal{G}} + O\left(\frac{C(\mathcal{F})^2C(\mathcal{G})^2}{p^{1/2}}\right).$$

1.9 Absolutely irreducible polynomials

In this section we discuss a notion called absolutely irreducible polynomial which we will use in Chapter 2.

Definition 1.7. *Let $\mathbb{F}_q$ be any field with q elements. A polynomial $f(x_1, x_2, ..., x_n) \in \mathbb{F}_q[x_1, x_2, ..., x_n]$ is called absolutely irreducible if it cannot be factored in a non-trivial manner in any algebraic extension of $\mathbb{F}_q$.*

For prime p consider the congruence

$$f(x_1, x_2, ..., x_n) \equiv 0 \pmod{p}, \tag{1.2}$$

where $f(x_1, x_2, ..., x_n) \in \mathbb{F}_p[x_1, x_2, ..., x_n]$.

S. Lang and A. Weil [30] showed that, if f is fixed and the prime modulus p varies, then the number N of solution of the congruence (1.2) becomes arbitrarily large as p increases and they even gave an estimate for the rate of increase of N. Their result can be formulated precisely as follows.

Theorem 1.2. *The number $N(f,p)$ of solutions of the congruence (1.2) satisfies the inequality*

$$|N(f,p) - p^{n-1}| < A(f)p^{n-1-(1/2)},$$

where $A(f)$ depends only on the polynomial f, not on p.

Lemma 1.3. *For a prime p, the polynomial $f(x,y) = (x-1)(y-1)(1-xy) - uxy \in \mathbb{F}_p[x,y]$, $u(\neq 0) \in \mathbb{F}_p$ is absolutely irreducible over $\mathbb{F}_p$.*

Proof. Consider $\mathbb{F}_q$, a finite extension of $\mathbb{F}_p$. Let the given polynomial be factored as,

$$(x-1)(y-1)(1-xy) - uxy = (S_1(y)x + T_1(y))(S_2(y)x + T_2(y)),$$

in $\mathbb{F}_q[x,y]$. Then comparing the coefficients of x, we get

$$\begin{aligned} S_1(y)S_2(y) &= y - y^2, \\ T_1(y)T_2(y) &= 1 - y, \\ S_1(y)T_2(y) + S_2(y)T_1(y) &= y^2 - uy - 1. \end{aligned}$$

If $S_1(y) = T_1(y) = (1-y)$ or $S_2(y) = T_2(y) = (1-y)$, then we have that $1-y$ divides $y^2 - uy - 1$, which is a contradiction. Hence we must have $S_1(y) = T_2(y) = (1-y)$ or $T_1(y) = S_2(y) = (1-y)$, which implies

$$\begin{aligned} (1-y)^2 + y &= y^2 - uy - 1 \\ \text{i.e., } y &= \frac{2}{1-u}, \end{aligned}$$

which is a contradiction. Hence the polynomial $f(x,y)$ must be absolutely irreducible over $\mathbb{F}_p$. ■

2

Fourth power mean of the 3-dimensional Kloosterman sum mod p

2.1 Introduction

In (1.1), we have defined hyper-Kloosterman sums $K(m, s; q)$, which are also called *higher-dimensional Kloosterman sums*. We define the *general higher-dimensional*

[1]The contents of this chapter have been accepted for publication in *Funct. Approx. Comment. Math* (2020).

Kloosterman sums $K(m, s, \chi; q)$ by

$$K(m, s, \chi; q) = \sum_{x_1=1}^{q}{}' \cdots \sum_{x_s=1}^{q}{}' \chi(x_1 \cdots x_s) \times e\left(\frac{x_1 + \cdots + x_s + m\overline{x_1 \cdots x_s}}{q}\right).$$

Here, $\sum_{x=1}^{q}{}'$ denotes the summation over all $1 \leq x \leq q$ such that $\gcd(x, q) = 1$, $e(y) = e^{2\pi iy}$, and $\overline{x}$ denotes the multiplicative inverse of x mod q, χ is a Dirichlet character mod q, m is any integer. Many authors studied the arithmetical properties of $K(m, s; p)$ and obtained a series of interesting results.

One such result is due to Mordell [33]. For odd prime p, he found the following estimate

$$|K(m, s; p)| \ll p^{\frac{s+1}{2}}.$$

Later P. Deligne [13] improved Mordell's result and obtained the upper bound estimate

$$|K(m, s; p)| \leq (s + 1)p^{\frac{s}{2}}. \tag{2.1}$$

There are many important applications of hyper-Kloosterman sums. One such is their occurrence in the study of automorphic forms. For instance, in [32], W. Luo, Z. Rudnick and P. Sarnak used the fact that powers of Gauss sums occur in the root number of the fundamental equation of certain automorphic L-functions, the inverse Mellin transform property and Deligne's bound to obtain a trivial estimate for the Langlands parameter of automorphic representations on GL_n. In addition, as for the classical Kloosterman sums, hyper-Kloosterman sums also occur in the spectral theory of GL_n automorphic forms. Later on many other results are obtained, see for example [31, 35, 36, 38].

In this chapter we will only concentrate on the general higher-dimensional Kloosterman sums. It is well known that for any principal character χ,

$$K(m,1,\chi;p) = -2\sqrt{p}\cos(\theta(m)),$$

for integer m, where the angle $\theta(m)$ is equidistributed in $[0,\pi]$ with respect to the Sato-Tate measure $\frac{2}{\pi}\sin^2(\theta)d\theta$. For example, see [23]. Thus moments can be estimated by evaluating the corresponding integral

$$\frac{1}{p-1}\sum_{m=1}^{p-1}|\frac{2}{\pi}\sin^2(\theta)d\theta|^{2\ell} \approx 2^{2\ell}p^{\ell}\frac{2}{\pi}\int_0^{\pi}\cos^{2\ell}(\theta)\sin^2(\theta)d\theta,$$

where ℓ is any positive integer. It would be interesting to investigate whether something similar is known for higher-dimensional generalized Kloosterman sums. In this chapter we study fourth power mean value of the *general s-dimensional Kloosterman sum*

$$\sum_{m=1}^{p-1}\sum_{\chi \bmod p}\left|\sum_{x_1=1}^{p-1}\cdots\sum_{x_s=1}^{p-1}\chi(x_1\cdots x_s)\cdot e\left(\frac{x_1+\cdots+x_s+m\overline{x_1\cdots x_s}}{p}\right)\right|^4. \tag{2.2}$$

2.2 Statement of the main result

In case of $s=1$, it is easy to evaluate (2.2). It can be easily seen that

$$\sum_{m=1}^{p-1}\sum_{\chi \bmod p}\left|\sum_{a=1}^{p-1}\chi(a)\cdot e\left(\frac{a+m\overline{a}}{p}\right)\right|^4 = 2p^4-8p^3+10p^2-3p-1.$$

For $s\geq 2$, Zhang and Li [41] first studied this sum and obtained an exact computational formula for (2.2) with $s=2$. For prime $p>3$, they proved the following

identity

$$\sum_{m=1}^{p-1}\sum_{\chi \bmod p}\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi(ab)\cdot e\left(\frac{a+b+m\overline{ab}}{p}\right)\right|^4$$
$$=(p-1)(2p^5-7p^4+2p^3+8p^2+4p+1).$$

Recently, Zhang and Lv [42] obtained the formula for $s=3$. For example, for $p>3$, they prove that

$$\sum_{m=1}^{p-1}\sum_{\chi \bmod p}\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\cdot e\left(\frac{a+b+c+m\overline{abc}}{p}\right)\right|^4=2p^8+O(p^{\frac{15}{2}}). \tag{2.3}$$

Here we improve the asymptotic formula (2.3). To be specific, we prove the following theorem.

Theorem 2.1. *For any prime $p>3$, we have*

$$\sum_{m=1}^{p-1}\sum_{\chi \bmod p}\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\cdot e\left(\frac{a+b+c+m\overline{abc}}{p}\right)\right|^4=2p^8+O(p^7).$$

2.3 Proof of Theorem 2.1

In [42, Lemma 2.2], Zhang and Lv found an estimate of a character sum and used it to prove the asymptotic formula (2.3). In the following lemma, we obtain a better estimate of the sum. In the proof we take an average of the number of $\mathbb{F}_p$-points on $(x-1)(y-1)(1-xy)-uxy=0$ over u, an idea due to Cochrane (see for example [10]). We denote the principal character by χ_0. The arguments in the proofs given in this chapter are variants of [42].

Lemma 2.2. *Let p be an odd prime. Then we have the identity*

$$\sum_{\substack{x_1=1}}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{y_1=1}^{p-1}\sum_{y_2=1}^{p-1}\sum_{\substack{y_3=1\\ x_1x_2x_3\equiv y_1y_2y_3 \pmod p\\ (x_1-1)(x_2-1)(x_3-1)\equiv(y_1-1)(y_2-1)(y_3-1) \pmod p}}^{p-1} \chi_0\left((\overline{x_1x_2x_3}-1)(x_1-1)(x_2-1)(x_3-1)\right)$$
$$= p^4 - 10p^3 + O(p^2).$$

Proof. Note that $\chi_0(n) = 1$ if $\gcd(n,p) = 1$ and $\chi_0(n) = 1$ if $p|n$. Hence, we have

$$\sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{y_1=1}^{p-1}\sum_{y_2=1}^{p-1}\sum_{\substack{y_3=1\\ \prod_{i=1}^3 x_i\equiv\prod_{i=1}^3 y_i \pmod p\\ \prod_{i=1}^3(x_i-1)\equiv\prod_{i=1}^3(y_i-1) \pmod p}}^{p-1} \chi_0\left((\overline{x_1x_2x_3}-1)(x_1-1)(x_2-1)(x_3-1)\right)$$
$$= M_1 - M_2 - M_3, \tag{2.4}$$

where

$$M_1 = \sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{y_1=1}^{p-1}\sum_{y_2=1}^{p-1}\sum_{\substack{y_3=1\\ \prod_{i=1}^3 x_i\equiv\prod_{i=1}^3 y_i \pmod p\\ \prod_{i=1}^3(x_i-1)\equiv\prod_{i=1}^3(y_i-1) \pmod p}}^{p-1} 1;$$

$$M_2 = \sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{y_1=1}^{p-1}\sum_{y_2=1}^{p-1}\sum_{\substack{y_3=1\\ \prod_{i=1}^3 x_i\equiv\prod_{i=1}^3 y_i\equiv 1 \pmod p\\ \prod_{i=1}^3(x_i-1)\equiv\prod_{i=1}^3(y_i-1) \pmod p}}^{p-1} 1;$$

$$M_3 = \sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{y_1=1}^{p-1}\sum_{y_2=1}^{p-1}\sum_{\substack{y_3=1\\ \prod_{i=1}^3 x_i\equiv\prod_{i=1}^3 y_i \pmod p\\ \prod_{i=1}^3(x_i-1)\equiv\prod_{i=1}^3(y_i-1)\equiv 0 \pmod p}}^{p-1} \chi_0\left(\overline{x_1x_2x_3}-1\right).$$

From [42, (2.4) and (2.9)], we know that

$$M_3 = \sum_{\substack{x_1=1}}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{y_1=1}^{p-1}\sum_{y_2=1}^{p-1}\sum_{y_3=1}^{p-1} \chi_0\left(\overline{x_1x_2x_3}-1\right) = 9(p-2)^3, \tag{2.5}$$
$$\prod_{i=1}^3 x_i \equiv \prod_{i=1}^3 y_i \pmod p$$
$$\prod_{i=1}^3 (x_i-1) \equiv \prod_{i=1}^3 (y_i-1) \equiv 0 \pmod p$$

$$M_1 = \sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{y_1=1}^{p-1}\sum_{y_2=1}^{p-1}\sum_{y_3=1}^{p-1} 1 = p^4 - 9p^2 + 5p + 11. \tag{2.6}$$
$$\prod_{i=1}^3 x_i \equiv \prod_{i=1}^3 y_i \pmod p$$
$$\prod_{i=1}^3 (x_i-1) \equiv \prod_{i=1}^3 (y_i-1) \pmod p$$

Next, we have

$$\begin{aligned} M_2 &= \sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{y_1=1}^{p-1}\sum_{y_2=1}^{p-1}\sum_{y_3=1}^{p-1} 1 \\ &\quad \prod_{i=1}^3 x_i \equiv \prod_{i=1}^3 y_i \equiv 1 \pmod p \\ &\quad \prod_{i=1}^3 (x_i-1) \equiv \prod_{i=1}^3 (y_i-1) \pmod p \\ &= \sum_{u=0}^{p-1} \left(\sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1} 1 \right)^2 \\ &\quad \prod_{i=1}^3 x_i \equiv 1 \pmod p,\ \prod_{i=1}^3 (x_i-1) \equiv u \pmod p \\ &= (3p-5)^2 + \sum_{u=1}^{p-1} \left(\sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1} 1 \right)^2 \\ &\quad \prod_{i=1}^2 (x_i-1)(\overline{x_1x_2}-1) \equiv u \pmod p \\ &= (3p-5)^2 + \sum_{u=1}^{p-1} \left(-2 + \sum_{x_1=0}^{p-1}\sum_{x_2=0}^{p-1} 1 \right)^2. \end{aligned} \tag{2.7}$$
$$(x_1-1)(x_2-1)(1-x_1x_2) - ux_1x_2 \equiv 0 \pmod p$$

We define $M(u)$ as the cardinality of the set

$$\{(x_1, x_2) \in \mathbb{F}_p^2 |\ x_1, x_2 \neq 0,\ (x_1-1)(x_2-1)(\overline{x_1x_2}-1) = u\}.$$

Consider the polynomial

$$f(x,y) = (x-1)(y-1)(1-xy) - uxy$$

in $\mathbb{F}_p[x,y]$. In Lemma 1.3, we have proved that the polynomial $f(x,y)$ is absolutely irreducible over $\mathbb{F}_p$, for any fixed $u \in \mathbb{F}_p \setminus \{0\}$. Hence from Theorem 1.2, we have

$$\sum_{\substack{x_1=0}}^{p-1}\sum_{x_2=0}^{p-1} \qquad 1 = p + E(u),$$
$$(x_1-1)(x_2-1)(1-x_1x_2)\equiv u x_1x_2 \pmod p$$

where $E(u) = O(\sqrt{p})$. Thus,

$$M(u) = \sum_{\substack{x_1=1}}^{p-1}\sum_{x_2=1}^{p-1} \qquad 1 = p - 2 + E(u). \tag{2.8}$$
$$(x_1-1)(x_2-1)(\overline{x_1x_2}-1)\equiv u \pmod p$$

Note that

$$\begin{aligned}\sum_{u=1}^{p-1} M(u) &= \#\{(x_1,x_2)\in\mathbb{F}_p^2 |\ x_1,x_2\neq 0,1;\ x_1x_2\neq 1\}\\ &= p^2-5p+6. \end{aligned}\tag{2.9}$$

Hence (2.8) and (2.9) yield

$$\begin{aligned}\sum_{u=1}^{p-1} E(u) &= p^2-5p+6-(p-1)(p-2)\\ &= -2p+4. \end{aligned}\tag{2.10}$$

From (2.8) and then using (2.10) and the fact that $E(u) = O(\sqrt{p})$, we obtain

$$\begin{aligned}\sum_{u=1}^{p-1}(M(u))^2 &= \sum_{u=1}^{p-1}(p-2)^2 + 2(p-2)\sum_{u=1}^{p-1}E(u) + \sum_{u=1}^{p-1}(E(u))^2\\ &= (p-1)(p^2-4p+4) + 2(p-2)(-2p+4) + O(p^2)\\ &= p^3 + O(p^2). \end{aligned}\tag{2.11}$$

Hence from (2.7) and (2.11) we get

$$M_2 = \sum_{\substack{x_1=1}}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{y_1=1}^{p-1}\sum_{y_2=1}^{p-1}\sum_{y_3=1}^{p-1} 1 = p^3 + O(p^2). \tag{2.12}$$
$$\substack{\prod_{i=1}^{3} x_i \equiv \prod_{i=1}^{3} y_i \equiv 1 \pmod p \\ \prod_{i=1}^{3}(x_i-1) \equiv \prod_{i=1}^{3}(y_i-1) \pmod p}$$

Combining (2.4), (2.5), (2.6), and (2.12) we obtain the required result. ■

Lemma 2.3 (Lemma 2.3 [42]). *Let p be an odd prime and χ be any character mod p. Then for primitive character χ_1 mod p, we have the identity*

$$\left|\sum_{m=1}^{p-1}\chi_1(m)\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\cdot e\left(\frac{a+b+c+m\overline{abc}}{p}\right)\right|^2\right|^2$$
$$= p^4\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\overline{\chi_1}((\overline{abc}-1)(a-1)(b-1)(c-1))\right|^2.$$

We now give a proof of Theorem 2.1.

Proof of Theorem 2.1. From the orthogonality property of characters mod p we have

$$\sum_{\chi \bmod p}\sum_{\chi_1 \bmod p}\left|\sum_{m=1}^{p-1}\chi_1(m)\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\cdot e\left(\frac{a+b+c+m\overline{abc}}{p}\right)\right|^2\right|^2$$
$$= (p-1)\sum_{m=1}^{p-1}\sum_{\chi \bmod p}\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\cdot e\left(\frac{a+b+c+m\overline{abc}}{p}\right)\right|^4. \tag{2.13}$$

Also we have

$$\sum_{\chi \bmod p}\sum_{\chi_1 \bmod p}\left|\sum_{m=1}^{p-1}\chi_1(m)\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\cdot e\left(\frac{a+b+c+m\overline{abc}}{p}\right)\right|^2\right|^2$$
$$= \sum_{\chi \bmod p}\sum_{\substack{\chi_1 \bmod p \\ \chi_1 \neq \chi_0}}\left|\sum_{m=1}^{p-1}\chi_1(m)\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\cdot e\left(\frac{a+b+c+m\overline{abc}}{p}\right)\right|^2\right|^2$$

$$+\sum_{\chi \bmod p}\left|\sum_{m=1}^{p-1}\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\cdot e\left(\frac{a+b+c+m\overline{abc}}{p}\right)\right|^2\right|^2. \tag{2.14}$$

From (3.3) of [42] we get

$$\begin{aligned}&\sum_{\chi \bmod p}\left|\sum_{m=1}^{p-1}\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\cdot e\left(\frac{a+b+c+m\overline{abc}}{p}\right)\right|^2\right|^2\\ &=(p-2)(p^4-2p^3-p^2-p)^2+(p^4-p^3-p^2-p-1)^2\\ &=(p-1)(p^8+O(p^7)).\end{aligned} \tag{2.15}$$

Now using Lemma 2.2 and Lemma 2.3 we have

$$\begin{aligned}&\sum_{\chi \bmod p}\sum_{\substack{\chi_1 \bmod p\\ \chi_1\neq\chi_0}}\left|\sum_{m=1}^{p-1}\chi_1(m)\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\cdot e\left(\frac{a+b+c+m\overline{abc}}{p}\right)\right|^2\right|^2\\ &=p^4(p-1)^2(p^4-10p^3+O(p^2))-p^4(p-1)(p-2)(p^2-5p+7)^2\\ &=(p-1)(p^8+O(p^7)).\end{aligned} \tag{2.16}$$

Combining (2.14), (2.15) and (2.16) we obtain

$$\begin{aligned}&\sum_{\chi \bmod p}\sum_{\chi_1 \bmod p}\left|\sum_{m=1}^{p-1}\chi_1(m)\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi(abc)\cdot e\left(\frac{a+b+c+m\overline{abc}}{p}\right)\right|^2\right|^2\\ &=(p-1)(p^8+O(p^7))+(p-1)(p^8+O(p^7))\\ &=(p-1)(2p^8+O(p^7)).\end{aligned} \tag{2.17}$$

Finally using (2.13) and (2.17), we complete the proof of our main theorem. ■

2.4 Concluding remarks

The Kloosterman sum $K(m, s, \chi; q)$ is defined for any modulus q. However, in the asymptotic formula (2.3) and Theorem 2.1, the Kloosterman sum is considered for prime modulus only. It would be interesting to extend Theorem 2.1 to any modulus q. It should be noted that the proof of Theorem 2.1 depends on the classical estimate of the number of points on the curve $(x-1)(y-1)(1-xy)-uxy = 0, u \neq 0$ over a finite field, which comes from Theorem 1.2 using the absolute irreducibility of the polynomial $(x-1)(y-1)(1-xy)-uxy$ over a finite field. Therefore, it may not be trivial to extend Theorem 2.1 to any modulus q.

3

Fourth power mean of the 4-dimensional Kloosterman sum mod p

3.1 Introduction and statement of the main result

In this chapter we study the fourth power mean value of the *general* 4*-dimensional Kloosterman sums*

$$\sum_{m=1}^{p-1}\sum_{\chi \bmod p}\left|\sum_{x_1=1}^{p-1}\cdots\sum_{x_4=1}^{p-1}\chi(x_1\cdots x_4)\cdot e\left(\frac{x_1+\cdots+x_4+m\overline{x_1\cdots x_4}}{p}\right)\right|^4. \tag{3.1}$$

[1]The contents of this chapter have been published in *Research in Number Theory* (2020).

For an odd prime p, using (2.1) with $s = 4$ and then taking summation over χ and m, one can find that

$$\sum_{m=1}^{p-1}\sum_{\chi \bmod p}\left|\sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{x_4=1}^{p-1}\chi(\prod_{i=1}^{4}x_i)e\left(\frac{\sum_{i=1}^{4}x_i+m\prod_{i=1}^{4}\overline{x_i}}{p}\right)\right|^4 \leq 5^4p^{10}. \quad (3.2)$$

Finding an asymptotic formula for (3.1) seems to be more difficult as the idea used in [42] to derive (2.3) is not sufficient to get a better estimate than (3.2). In the following theorem we find an asymptotic formula for (3.1). To be specific, we prove the following.

Theorem 3.1. *For any prime $p > 3$, we have*

$$\sum_{m=1}^{p-1}\sum_{\chi \bmod p}\left|\sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{x_4=1}^{p-1}\chi(\prod_{i=1}^{4}x_i)e\left(\frac{\sum_{i=1}^{4}x_i+m\prod_{i=1}^{4}\overline{x_i}}{p}\right)\right|^4 = 2p^{10}+O(p^9).$$

Throughout this chapter, $\sum_{X}$ and $\sum_{X'}$ denote the sums $\sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{x_4=1}^{p-1}$ and $\sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}$, respectively. Similarly, we use the notation $\sum_{Y}$ and $\sum_{Y'}$, where Y denotes the 4-tuples (y_1, y_2, y_3, y_4) and Y' denotes the 3-tuples (y_1, y_2, y_3) with $1 \leq y_i \leq p-1$ for all i. We denote the principal character by χ_0 which is defined as $\chi_0(n) = 1$, if $\gcd(n, p) = 1$; and $\chi_0(n) = 0$, if $p|n$.

3.2 Some congruence equations modulo p

In this section we find the number of solutions to some congruences modulo p.

Lemma 3.2. *Let p be an odd prime. Let S_1 be the set of solutions in $(\mathbb{F}_p^{\times})^7$ of the following congruences modulo p:*

$$x_1x_2x_3x_4 \equiv y_1y_2y_3, \ \prod_{i=1}^{4}(x_i-1) \equiv 0, \ \prod_{i=1}^{3}(x_i-1) \equiv \prod_{i=1}^{3}(y_i-1).$$

Then the number of elements in the set S_1 is given by

$$|S_1| = 10p^4 - 63p^3 + 159p^2 - 199p + 107.$$

Proof. We have

$$|S_1| = \sum_{\substack{X' \\ \prod_{i=1}^3 x_i \equiv \prod_{i=1}^3 y_i \pmod p \\ \prod_{i=1}^3 (x_i-1) \equiv \prod_{i=1}^3 (y_i-1) \pmod p}} \sum_{Y'} 1 + \sum_{\substack{X' \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^3 y_i \pmod p \\ \prod_{i=1}^3 (x_i-1) \equiv 0 \pmod p \\ \prod_{i=1}^3 (x_i-1) \equiv \prod_{i=1}^3 (y_i-1) \pmod p}} \sum_{x_4=2}^{p-1} \sum_{Y'} 1. \tag{3.3}$$

From [42, (2.9)] we have

$$\sum_{\substack{X' \\ \prod_{i=1}^3 x_i \equiv \prod_{i=1}^3 y_i \pmod p \\ \prod_{i=1}^3 (x_i-1) \equiv \prod_{i=1}^3 (y_i-1) \pmod p}} \sum_{Y'} 1 = p^4 - 9p^2 + 5p + 11. \tag{3.4}$$

Also, the second sum can be written as

$$\begin{aligned} &\sum_{\substack{X' \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^3 y_i \pmod p \\ \prod_{i=1}^3 (x_i-1) \equiv 0 \pmod p \\ \prod_{i=1}^3 (x_i-1) \equiv \prod_{i=1}^3 (y_i-1) \pmod p}} \sum_{x_4=2}^{p-1} \sum_{Y'} 1 \\ &= 3 \sum_{\substack{x_1=2 \\ x_1 x_2 x_4 \equiv y_1 y_2 y_3 \pmod p \\ \prod_{i=1}^3 (y_i-1) \equiv 0 \pmod p}}^{p-1} \sum_{x_2=2}^{p-1} \sum_{x_4=2}^{p-1} \sum_{Y'} 1 + 3 \sum_{\substack{x_1=2 \\ x_1 x_4 \equiv y_1 y_2 y_3 \pmod p \\ \prod_{i=1}^3 (y_i-1) \equiv 0 \pmod p}}^{p-1} \sum_{x_4=2}^{p-1} \sum_{Y'} 1 + \sum_{\substack{x_4=2 \\ x_4 \equiv y_1 y_2 y_3 \pmod p \\ \prod_{i=1}^3 (y_i-1) \equiv 0 \pmod p}}^{p-1} \sum_{Y'} 1. \end{aligned} \tag{3.5}$$

To calculate (3.5), we first note the following three sums:

$$\sum_{\substack{a_1=2 \\ a_1 a_2 a_3 \equiv 1 \pmod p}}^{p-1} \sum_{a_2=2}^{p-1} \sum_{a_3=2}^{p-1} 1 = (p-1)^2 - 3(p-2) - 1, \tag{3.6}$$

which gives

$$\begin{aligned}&\sum_{\substack{a_1=2\\a_1a_2a_3a_4\equiv 1 \pmod p}}^{p-1}\sum_{a_2=2}^{p-1}\sum_{a_3=2}^{p-1}\sum_{a_4=2}^{p-1}1\\&=(p-1)^3-4[(p-1)^2-3(p-2)-1]-6(p-2)-1\\&=p^3-7p^2+17p-14,\end{aligned}\tag{3.7}$$

and it finally yields,

$$\sum_{\substack{a_1=2\\a_1a_2a_3a_4a_5\equiv 1 \pmod p}}^{p-1}\sum_{a_2=2}^{p-1}\sum_{a_3=2}^{p-1}\sum_{a_4=2}^{p-1}\sum_{a_5=2}^{p-1}1=p^4-9p^3+31p^2-49p+30.\tag{3.8}$$

Using (3.6), (3.7) and (3.8) we find that

$$\begin{aligned}&\sum_{\substack{x_1=2\\x_1x_2x_4\equiv y_1y_2y_3 \pmod p\\\prod_{i=1}^3(y_i-1)\equiv 0 \pmod p}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_4=2}^{p-1}\sum_{Y'}1\\&=3\sum_{\substack{x_1=2\\x_1x_2x_4\equiv y_2y_3 \pmod p}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_4=2}^{p-1}\sum_{y_2=2}^{p-1}\sum_{y_3=2}^{p-1}1+3\sum_{\substack{x_1=2\\x_1x_2x_4\equiv y_3 \pmod p}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_4=2}^{p-1}\sum_{y_3=2}^{p-1}1+\sum_{\substack{x_1=2\\x_1x_2x_4\equiv 1 \pmod p}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_4=2}^{p-1}1\\&=3p^4-24p^3+73p^2-101p+54,\end{aligned}\tag{3.9}$$

$$\begin{aligned}\sum_{\substack{x_1=2\\x_4x_1\equiv y_1y_2y_3 \pmod p\\\prod_{i=1}^3(y_i-1)\equiv 0 \pmod p}}^{p-1}\sum_{x_4=2}^{p-1}\sum_{Y'}1&=3\sum_{\substack{x_1=2\\x_4x_1\equiv y_2y_3 \pmod p}}^{p-1}\sum_{x_4=2}^{p-1}\sum_{y_2=2}^{p-1}\sum_{y_3=2}^{p-1}1+3\sum_{\substack{x_1=2\\x_4x_1\equiv y_3 \pmod p}}^{p-1}\sum_{x_4=2}^{p-1}\sum_{y_3=2}^{p-1}1+\sum_{\substack{x_1=2\\x_4x_1\equiv 1 \pmod p}}^{p-1}\sum_{x_4=2}^{p-1}1\\&=3p^3-18p^2+37p-26,\end{aligned}\tag{3.10}$$

and

$$\sum_{\substack{x_4=2 \\ x_4\equiv y_1y_2y_3 \pmod p \\ \prod_{i=1}^{3}(y_i-1)\equiv 0 \pmod p}}^{p-1} \sum_{Y'} 1 = 3\sum_{\substack{x_4=2 \\ x_4\equiv y_2y_3 \pmod p}}^{p-1}\sum_{y_2=2}^{p-1}\sum_{y_3=2}^{p-1} 1 + 3\sum_{\substack{x_4=2 \\ x_4\equiv y_3 \pmod p}}^{p-1}\sum_{y_3=2}^{p-1} 1 = 3p^2 - 12p + 12. \tag{3.11}$$

Employing (3.9), (3.10) and (3.11) into (3.5), we obtain

$$\sum_{\substack{X' \\ \prod_{i=1}^{4} x_i\equiv\prod_{i=1}^{3} y_i \pmod p \\ \prod_{i=1}^{3}(x_i-1)\equiv 0 \pmod p \\ \prod_{i=1}^{3}(x_i-1)\equiv\prod_{i=1}^{3}(y_i-1) \pmod p}} \sum_{x_4=2}^{p-1} \sum_{Y'} 1 = 9p^4 - 63p^3 + 168p^2 - 204p + 96. \tag{3.12}$$

We now complete the proof by combining (3.3), (3.4) and (3.12). ■

Lemma 3.3. *Let p be an odd prime and S_2 be the set of solutions in $(\mathbb{F}_p^\times)^7$ of the following two congruences modulo p:*

$$x_1x_2x_3x_4 \equiv y_1y_2y_3, \quad \prod_{i=1}^{3}(x_i - 1) \equiv \prod_{i=1}^{3}(y_i - 1).$$

Then we have

$$|S_2| = p^5 - 2p^4 - 5p^3 + 12p^2 + 3p - 13.$$

Proof. For $0 \le u \le p-1$, let $S(u)$ denote the number of solutions of

$$\prod_{i=1}^{3}(x_i - 1) \equiv u \pmod p,$$

where $x_i \in \mathbb{F}_p^\times$ for $i = 1, 2, 3$. For $u = 0$ we count solutions with exactly one, two and three of the $x_i = 1$, to get

$$S(0) = 3(p-2)^2 + 3(p-2) + 1 = 3p^2 - 9p + 7.$$

For $u = p-1$, x_1 and x_2 can freely run through $p-2$ values, except for the $p-2$ pairs (x_1, x_2) where solving for x_3 gives $x_3 = 0$. Thus

$$S(p-1) = (p-2)^2 - (p-2) = p^2 - 5p + 6.$$

Finally, for $1 \leq u < p-1$, x_1 and x_2 can freely run through $p-2$ values except for the $p-3$ pairs (x_1, x_2) giving $x_3 = 0$. Thus, for $1 \leq u < p-1$, we have

$$S(u) = (p-2)^2 - (p-3) = p^2 - 5p + 7.$$

For any choice of $x_1, x_2, x_3, y_1, y_2, y_3$; x_4 is uniquely determined by the first equation $x_1x_2x_3x_4 \equiv y_1y_2y_3 \pmod{p}$. Therefore

$$\begin{aligned} |S_2| = \sum_{u=0}^{p-1} S(u)^2 &= (3p^2 - 9p + 7)^2 + (p^2 - 5p + 6)^2 + (p-2)(p^2 - 5p + 7)^2 \\ &= p^5 - 2p^4 - 5p^3 + 12p^2 + 3p - 13. \end{aligned}$$

This completes the proof of the lemma. ■

3.3 A result of P. Deligne

The following lemma is due to P. Deligne. He communicated the proof to us through an email. Here we present a brief sketch of the proof. His entire proof is given in the Appendix.

Lemma 3.4. *Let p be an odd prime and $1 \leq u \leq p-1$. Then the number of $\mathbb{F}_p$-points on the surface $(x-1)(y-1)(z-1)(1-xyz) - uxyz = 0$ is given by*

$$\begin{aligned} &|\{(x, y, z) \in \mathbb{F}_p^3 : (x-1)(y-1)(z-1)(1-xyz) - uxyz = 0\}| \\ &= p^2 + \mathrm{Tr}(\mathrm{Frob}\ V_u) + 7. \end{aligned}$$

Here, $\mathrm{Tr}(\mathrm{Frob}\ V_u)$ *denotes the trace of the Frobenius endomorphism, where* V_u *is a part of the cohomology on the surface*

$$(x-1)(y-1)(z-1)(1-xyz) - uxyz = 0.$$

Also, $|\mathrm{Tr}(\mathrm{Frob}\ V_u)| \leq 4p$.

Proof. On the surface

$$(x-1)(y-1)(z-1)(1-xyz) - uxyz = 0, u \neq 0, \tag{3.13}$$

we have the six lines where one coordinate is 0, equivalently one coordinate is 1. They meet in the six points which are S_3-conjugate of $(0,0,1)$ or $(1,1,0)$, where two lines meet. The union of the six lines has hence $6p-6$ points. If we remove them, and put $t = \frac{1}{xyz}$, we have the symmetric form in $\mathbb{G}_m^4$, defined as

$$\begin{aligned} xyzt &= 1; \\ (x-1)(y-1)(z-1)(t-1) &= u, \end{aligned} \tag{3.14}$$

where the four coordinates play symmetric role. Here $\mathbb{G}_m = \mathbb{P}^1 - \{0, \infty\}$. In $\mathbb{G}_m^4$ we have the additional symmetry

$$\tau : (x,y,z,t) \longrightarrow (\frac{1}{x}, \frac{1}{y}, \frac{1}{z}, \frac{1}{t}).$$

To compactify, preserving the symmetry, one should embed $\mathbb{G}_m^4$ into $(\mathbb{P}^1)^4$. If on the i-th $\mathbb{P}^1$ we use projective coordinates (x_i, x_i'), then (3.14) is the trace on $\mathbb{G}_m^4 \subset (\mathbb{P}^1)^4$

of the intersection of the hypersurfaces with the equations:

$$\begin{aligned} \prod_{i=1}^{4} x_i &= \prod_{i=1}^{4} x_i'; \\ \prod_{i=1}^{4} (x_i - x_i') &= u \prod_{i=1}^{4} x_i'. \end{aligned} \tag{3.15}$$

In these coordinates, τ is $x_i \leftrightarrow x_i'$.

On $\mathbb{P}^1$, with homogeneous coordinates x, x', $x = 0$ defines the point 0, $x' = 0$ the point ∞ and $x - x' = 0$ the point 1. If $(P_1, P_2, P_3, P_4) \in (\mathbb{P}^1)^4$ is on the surface (3.15), one P_i is 0 if and only if one other is 1 if and only if a third is ∞. One obtains the surface (3.14) from the surface (3.15) by removing the $\mathbb{P}^1$ in the S_4-orbit of $\{0\} \times \{1\} \times \{\infty\} \times \mathbb{P}^1 \subset (\mathbb{P}^1)^4$. The set of twenty four $\mathbb{P}^1$ is a homogeneous space under the symmetry group $S_4 \times \{1, \tau\}$. To obtain the surface (3.13), one removes only 18 of the 24 lines: one takes the intersection with

$$(\mathbb{P}^1 - \{\infty\}) \times (\mathbb{P}^1 - \{\infty\}) \times (\mathbb{P}^1 - \{\infty\}) \times (\mathbb{P}^1 - \{0\}).$$

This means putting $x_1' = x_2' = x_3' = x_4 = 1$ and one takes as coordinates x_1, x_2, x_3, x_4'. The equations become

$$\begin{aligned} x_1 x_2 x_3 &= x_4'; \\ (x_1 - 1)(x_2 - 1)(x_3 - 1)(1 - x_4') &= u x_4', \end{aligned}$$

which, eliminating x_4', gives (3.13). The lines among the twenty four $\mathbb{P}^1$ which persist in (3.13) are those mapping to ∞ in the 4th $\mathbb{P}^1$.

The surface (3.15) is non-singular except for $u = 16$ or $u = -4$. In case of $u = 16$, the singular point is $(-1, -1, -1, -1)$, and when $u = -4$, $\pm(i, i, i, i)$ are the singular points, where $i = \sqrt{-1}$. These points are contained in $\mathbb{G}_m^4$. This is checked using the Jacobian criterion. Outside of $\mathbb{G}_m^4$, we have the 24 projective

lines $(P_1, P_2, P_3, P_4) \in (\mathbb{P}^1)^4$ where some three of the P_i are $0, 1, \infty$. They are simply transitively permuted by S_4. We also have the symmetry $z \mapsto z^{-1}$ on all $\mathbb{P}^1$. To check non singularity outside of $\mathbb{G}_m^4$, it hence suffices to see it on the affine line of $(0, 1, \infty, t)$, $t \neq \infty$.

If in $(\mathbb{P}^1)^4$, we take the intersection of two hypersurfaces of degree $(1, 1, 1, 1)$, we get a $K3$ surface (when non-singular). Hence the surface (3.15) is a $K3$ surface, except for $u \neq 16, -4$. In the intersections, we have 36 points, the coordinates $0, 1, \infty$, all three occuring, one of them twice. Thus, over $\mathbb{F}_p$, we have:

$$\begin{aligned}
&\text{number of points on (3.13)} = \text{number of points on (3.14)} + 6p - 6;\\
&\text{number of points on (3.15)} = \text{number of points on (3.14)} + 24(p+1) - 36\\
&\qquad\qquad = \text{number of points on (3.14)} + 24p - 12.
\end{aligned}$$

To find the number of points on the surface (3.15), we will now study certain cohomology groups. The action of the symmetry group $S_4 \times \{1, \tau\}$ breaks the second cohomology group H^2 of the surface (3.15) into pieces indexed by the irreducible representations of the symmetry group. All the representations of S_4 in H^2 with a fixed vector by S_2 are contained in the span of the class of the 24 lines outside $\mathbb{G}_m^4$. This span is the image of a regular representation of S_4. The span of the 24 lines is of dimension 18, and τ acts on it with trace 0 because τ has no fixed points on the hypersurface (3.15) (for $u \neq 16$). As H^0 and H^4 contribute each 1 to the trace, the part of cohomology H^2 orthogonal to the 24 lines, as a representation, is

$$1\times \begin{array}{|c|}\hline\\\hline\\\hline\\\hline\end{array}\ (\tau = 1) \quad + \quad 3\times \begin{array}{|c|}\hline\\\hline\\\hline\\\hline\end{array}\ (\tau = -1) \tag{3.16}$$

To count points on the surface (3.15) over $\mathbb{F}_p$, one then needs to know the eigenvalues of the Frobenius. On the span of the 24 lines, the eigenvalue of Frobenius is p. On

the class of the first representation appearing in (3.16), the eigenvalue of Frobenius is $\pm p$. On the remaining orthogonal, we only know it is an orthogonal similitude with the standard bilinear form multiplied by p^2. Thus, the cardinality of $\mathbb{F}_p$-points on the given surface (3.13) is equal to $p^2 + \mathrm{Tr}(\mathrm{Frob}\ V_u) + 7$, where V_u is the orthogonal in H^2 of the span of the 24 lines and $|\mathrm{Tr}(\mathrm{Frob}\ V_u)| \leq 4p$. ■

3.4 Some lemmas

Using the result of P. Deligne and cardinalities of the sets S_1 and S_2 we now prove the next lemma. In the proof we take an average of the number of $\mathbb{F}_p$-points on the surface $(x-1)(y-1)(z-1)(1-xyz) - uxyz = 0$ over u.

Lemma 3.5. *Let p be an odd prime. Then we have the identity*

$$\sum_{\substack{X}}\sum_{\substack{Y \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^4 y_i \pmod p \\ \prod_{i=1}^4 (x_i-1) \equiv \prod_{i=1}^4 (y_i-1) \pmod p}} \chi_0\left((\overline{x_1x_2x_3x_4} - 1)(x_1-1)(x_2-1)(x_3-1)(x_4-1)\right) = p^6 - 15p^5 + 97p^4 + O(p^3).$$

Proof. We have

$$\sum_{\substack{X}}\sum_{\substack{Y \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^4 y_i \pmod p \\ \prod_{i=1}^4 (x_i-1) \equiv \prod_{i=1}^4 (y_i-1) \pmod p}} \chi_0\left((\overline{x_1x_2x_3x_4} - 1)(x_1-1)(x_2-1)(x_3-1)(x_4-1)\right) = N_1 - N_2 - N_3, \tag{3.17}$$

where

$$N_1 = \sum_{\substack{X}}\sum_{\substack{Y \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^4 y_i \pmod p \\ \prod_{i=1}^4 (x_i-1) \equiv \prod_{i=1}^4 (y_i-1) \pmod p}} 1;$$

$$N_2 = \sum_{\substack{X}}\sum_{\substack{Y \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^4 y_i \equiv 1 \pmod p \\ \prod_{i=1}^4 (x_i-1) \equiv \prod_{i=1}^4 (y_i-1) \pmod p}} 1;$$

$$N_3 = \sum_{\substack{X}}\sum_{\substack{Y \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^4 y_i \pmod p \\ \prod_{i=1}^4 (x_i-1) \equiv \prod_{i=1}^4 (y_i-1) \equiv 0 \pmod p}} \chi_0\left(\overline{x_1x_2x_3x_4} - 1\right).$$

Replacing x_4 with x_4y_4 we see that the number of solutions in $(\mathbb{F}_p^\times)^8$ of the congruences $\prod_{i=1}^4 x_i \equiv \prod_{i=1}^4 y_i \pmod p$ and $\prod_{i=1}^4 (x_i - 1) \equiv \prod_{i=1}^4 (y_i - 1) \pmod p$ is equal to the number of solutions of the congruences $\prod_{i=1}^4 x_i \equiv \prod_{i=1}^3 y_i \pmod p$ and $y_4(x_1x_2x_4+x_1x_3x_4+x_2x_3x_4-x_1x_4-x_2x_4-x_3x_4+x_4-y_1y_2-y_1y_3-y_2y_3+y_1+y_2+y_3-1) \equiv -x_1x_2x_3+x_1x_2+x_1x_3+x_2x_3-x_1-x_2-x_3+y_1y_2y_3-y_1y_2-y_1y_3-y_2y_3+y_1+y_2+y_3 \pmod p$. Hence we get

$$N_1 = \sum_{\substack{X}}\sum_{\substack{Y' \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^3 y_i \pmod p \\ \gcd(x_1x_2x_4+x_1x_3x_4+x_2x_3x_4-x_1x_4-x_2x_4-x_3x_4 \\ +x_4-y_1y_2-y_1y_3-y_2y_3+y_1+y_2+y_3-1,p)=1 \\ \gcd(-x_1x_2x_3+x_1x_2+x_1x_3+x_2x_3-x_1-x_2-x_3 \\ +y_1y_2y_3-y_1y_2-y_1y_3-y_2y_3+y_1+y_2+y_3,p)=1}} 1 + (p-1) \sum_{\substack{X}}\sum_{\substack{Y' \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^3 y_i \pmod p \\ x_1x_2x_4+x_1x_3x_4+x_2x_3x_4+x_4+y_1+y_2+y_3 \\ \equiv x_1x_4+x_2x_4+x_3x_4+y_1y_2+y_1y_3+y_2y_3+1 \pmod p \\ x_1x_2+x_1x_3+x_2x_3+y_1y_2y_3+y_1+y_2+y_3 \\ \equiv x_1x_2x_3+x_1+x_2+x_3+y_1y_2+y_1y_3+y_2y_3 \pmod p}} 1$$

$$= (p-1)^6 - N_4 - N_5 + pN_6,$$

where

$$N_4 = \sum_{\substack{X}}\sum_{\substack{Y' \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^3 y_i \pmod p \\ x_1x_2x_4+x_1x_3x_4+x_2x_3x_4+x_4+y_1+y_2+y_3 \\ \equiv x_1x_4+x_2x_4+x_3x_4+y_1y_2+y_1y_3+y_2y_3+1 \pmod p}} 1;$$

$$N_5 = \sum_{\substack{X}}\sum_{\substack{Y' \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^3 y_i \pmod p \\ x_1x_2+x_1x_3+x_2x_3+y_1y_2y_3+y_1+y_2+y_3 \\ \equiv x_1x_2x_3+x_1+x_2+x_3+y_1y_2+y_1y_3+y_2y_3 \pmod p}} 1;$$

$$N_6 = \sum_{X}\sum_{Y'} 1.$$
$$\prod_{i=1}^{4} x_i \equiv \prod_{i=1}^{3} y_i \pmod p$$
$$x_1x_2x_4+x_1x_3x_4+x_2x_3x_4+x_4+y_1+y_2+y_3 \equiv x_1x_4+x_2x_4+x_3x_4+y_1y_2+y_1y_3+y_2y_3+1 \pmod p$$
$$x_1x_2+x_1x_3+x_2x_3+y_1y_2y_3+y_1+y_2+y_3 \equiv x_1x_2x_3+x_1+x_2+x_3+y_1y_2+y_1y_3+y_2y_3 \pmod p$$

Note that the system of equations $\prod_{i=1}^{4} x_i \equiv \prod_{i=1}^{3} y_i \pmod p$, $x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 + x_4 + y_1 + y_2 + y_3 \equiv x_1x_4 + x_2x_4 + x_3x_4 + y_1y_2 + y_1y_3 + y_2y_3 + 1 \pmod p$ and $x_1x_2 + x_1x_3 + x_2x_3 + y_1y_2y_3 + y_1 + y_2 + y_3 \equiv x_1x_2x_3 + x_1 + x_2 + x_3 + y_1y_2 + y_1y_3 + y_2y_3 \pmod p$ is equivalent to the system of equations defining S_1 in Lemma 3.2. The system of equations $\prod_{i=1}^{4} x_i \equiv \prod_{i=1}^{3} y_i \pmod p$ and $x_1x_2 + x_1x_3 + x_2x_3 + y_1y_2y_3 + y_1 + y_2 + y_3 \equiv x_1x_2x_3 + x_1 + x_2 + x_3 + y_1y_2 + y_1y_3 + y_2y_3 \pmod p$ is equivalent to the system of equations defining S_2 in Lemma 3.3. Also, if we replace x_i with x_i^{-1} and y_i with y_i^{-1} for all i, the system of equations $\prod_{i=1}^{4} x_i \equiv \prod_{i=1}^{3} y_i \pmod p$ and $x_1x_2x_4+x_1x_3x_4+x_2x_3x_4+x_4+y_1+y_2+y_3 \equiv x_1x_4+x_2x_4+x_3x_4+y_1y_2+y_1y_3+y_2y_3+1 \pmod p$ becomes the system of equations defining S_2. So we have $N_6 = |S_1|$ and $N_4 = N_5 = |S_2|$. Hence, employing Lemma 3.2 and 3.3 we deduce that

$$N_1 = \sum_{X}\sum_{Y} 1 = (p-1)^6 - 2|S_2| + p|S_1|$$
$$\prod_{i=1}^{4} x_i \equiv \prod_{i=1}^{4} y_i \pmod p$$
$$\prod_{i=1}^{4} (x_i-1) \equiv \prod_{i=1}^{4} (y_i-1) \pmod p$$
$$= p^6 + 2p^5 - 44p^4 + 149p^3 - 208p^2 + 95p + 27. \tag{3.18}$$

Next, we have

$$N_2 = \sum_{X}\sum_{Y} 1$$
$$\prod_{i=1}^{4} x_i \equiv \prod_{i=1}^{4} y_i \equiv 1 \pmod p$$
$$\prod_{i=1}^{4} (x_i-1) \equiv \prod_{i=1}^{4} (y_i-1) \pmod p$$

$$
\begin{aligned}
&= \sum_{u=0}^{p-1} \left(\sum_{\substack{X \\ \prod_{i=1}^{4} x_i \equiv 1 \pmod p,\ \prod_{i=1}^{4}(x_i-1)\equiv u \pmod p}} 1 \right)^2 \\
&= (4p^2-14p+13)^2 + \sum_{u=1}^{p-1} \left(\sum_{\substack{x_1=1}}^{p-1} \sum_{x_2=1}^{p-1} \sum_{x_3=1}^{p-1} \sum_{\substack{ \\ \prod_{i=1}^{3}(x_i-1)(\overline{x_1x_2x_3}-1)\equiv u \pmod p}} 1 \right)^2 \\
&= (4p^2-14p+13)^2 + \sum_{u=1}^{p-1} \left(6-6p + \sum_{x_1=0}^{p-1} \sum_{x_2=0}^{p-1} \sum_{x_3=0}^{p-1} \sum_{\substack{ \\ \prod_{i=1}^{3}(x_i-1)(1-x_1x_2x_3)-ux_1x_2x_3 \\ \equiv 0 \pmod p}} 1 \right)^2
\end{aligned} \tag{3.19}
$$

We define $N(u)$ as the cardinality of the set

$$\{(x_1,x_2,x_3)|\ x_i \neq 0,\ 1 \leq i \leq 3,\ (x_1-1)(x_2-1)(x_3-1)(\overline{x_1x_2x_3}-1) = u\}.$$

Then from Lemma 3.4 and (3.19) we get

$$N(u) = p^2 - 6p + 13 + \mathrm{Tr}(\mathrm{Frob}\ V_u). \tag{3.20}$$

Note that

$$
\begin{aligned}
\sum_{u=1}^{p-1} N(u) &= \#\{(x_1,x_2,x_3)|\ x_1,x_2,x_3 \neq 0,1;\ x_1x_2x_3 \neq 1\} \\
&= p^3 - 7p^2 + 17p - 14.
\end{aligned} \tag{3.21}
$$

Hence combining (3.20) and (3.21) we obtain

$$\sum_{u=1}^{p-1} \mathrm{Tr}(\mathrm{Frob}\ V_u) = p^3 - 7p^2 + 17p - 14 - (p-1)(p^2-6p+13)$$

$$= -2p - 1. \tag{3.22}$$

Thus from (3.20) and using the fact that $|\mathrm{Tr}(\mathrm{Frob}\ V_u)| \leq 4p$ from Lemma 3.4 we obtain

$$\begin{aligned}
&\sum_{u=1}^{p-1}(N(u))^2 \\
&= \sum_{u=1}^{p-1}(p^2-6p+13)^2 + 2(p^2-6p+13)\sum_{u=1}^{p-1}\mathrm{Tr}(\mathrm{Frob}\ V_u) + \sum_{u=1}^{p-1}(\mathrm{Tr}(\mathrm{Frob}\ V_u))^2 \\
&= (p-1)(p^2-6p+13)^2 + 2(p^2-6p+13)(-2p-1) + O(p^3) \\
&= (p-1)(p^2-6p+13)^2 + O(p^3).
\end{aligned} \tag{3.23}$$

Now, (3.19) and (3.23) yield

$$N_2 = \sum_{\substack{X}}\sum_{\substack{Y \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^4 y_i \equiv 1 \pmod p \\ \prod_{i=1}^4 (x_i-1) \equiv \prod_{i=1}^4 (y_i-1) \pmod p}} 1 = p^5 + 3p^4 + O(p^3). \tag{3.24}$$

Finally, from the properties of reduced residue system mod p we have

$$\begin{aligned}
N_3 &= \sum_{\substack{X}}\sum_{\substack{Y \\ \prod_{i=1}^4 x_i \equiv \prod_{i=1}^4 y_i \pmod p \\ \prod_{i=1}^4 (x_i-1) \equiv \prod_{i=1}^4 (y_i-1) \equiv 0 \pmod p}} \chi_0\left(\overline{x_1x_2x_3x_4} - 1\right) \\
&= \sum_{u=2}^{p-1}\left(\sum_{\substack{X \\ \prod_{i=1}^4 x_i \equiv u \pmod p,\ \prod_{i=1}^4 (x_i-1) \equiv 0 \pmod p}} 1\right)^2 \\
&= \sum_{u=2}^{p-1}\left(4\sum_{\substack{x_2=2}}^{p-1}\sum_{x_3=2}^{p-1}\sum_{\substack{x_4=2 \\ x_2x_3x_4 \equiv u \pmod p}}^{p-1} 1 + 6\sum_{x_3=2}^{p-1}\sum_{\substack{x_4=2 \\ x_3x_4 \equiv u \pmod p}}^{p-1} 1 + 4\sum_{\substack{x_4=2 \\ x_4 \equiv u \pmod p}}^{p-1} 1\right)^2
\end{aligned}$$

$$= \sum_{u=2}^{p-1}\left(4\sum_{\substack{x_2=1\\ x_2x_3x_4\equiv u \pmod p}}^{p-1}\sum_{x_3=1}^{p-1}\sum_{x_4=1}^{p-1}1 - 6\sum_{\substack{x_3=2\\ x_3x_4\equiv u \pmod p}}^{p-1}\sum_{x_4=2}^{p-1}1 - 8\sum_{\substack{x_4=2\\ x_4\equiv u \pmod p}}^{p-1}1\right)^2$$
$$= (p-2)(4p^2-14p+14)^2. \tag{3.25}$$

Combining (3.17), (3.18), (3.24) and (3.25) we obtain the required result. ■

Lemma 3.6. *Let p be an odd prime. Then we have*

$$\sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}\sum_{x_4=2}^{p-1}\sum_{y_1=2}^{p-1}\sum_{y_2=2}^{p-1}\sum_{y_3=2}^{p-1}\sum_{y_4=2}^{p-1}\chi_0(x_1x_2x_3x_4-1)$$
$$\prod_{i=1}^4 x_i\equiv\prod_{i=1}^4 y_i \pmod p$$
$$= p^7-16p^6+111p^5-434p^4+1035p^3-1508p^2+1245p-450.$$

Proof. We have

$$\sum_{x_1=2}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}\sum_{x_4=2}^{p-1}\sum_{y_1=2}^{p-1}\sum_{y_2=2}^{p-1}\sum_{y_3=2}^{p-1}\sum_{y_4=2}^{p-1}\chi_0(x_1x_2x_3x_4-1)$$
$$\prod_{i=1}^4 x_i\equiv\prod_{i=1}^4 y_i \pmod p$$
$$=\sum_{u=2}^{p-1}\left(\sum_{\substack{x_1=2\\ \prod_{i=1}^4 x_i\equiv u \pmod p}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}\sum_{x_4=2}^{p-1}1\right)^2. \tag{3.26}$$

Notice that, for $u\neq 1$

$$\sum_{\substack{x_1=1}}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{x_4=1}^{p-1}1 = \sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}\sum_{x_4=2}^{p-1}1 + 4\sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}1 + 6\sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}1 + 4\sum_{x_1=2}^{p-1}1$$
$$\prod_{i=1}^4 x_i\equiv u \pmod p \quad \prod_{i=1}^4 x_i\equiv u \pmod p \quad \prod_{i=1}^3 x_i\equiv u \pmod p \quad \prod_{i=1}^2 x_i\equiv u \pmod p \quad x_1\equiv u \pmod p$$

and

$$\sum_{\substack{x_1=1}}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}1 = \sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}1 + 3\sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}1 + 3\sum_{\substack{x_1=2\\ x_1\equiv u \pmod p}}^{p-1}1.$$
$$\prod_{i=1}^3 x_i\equiv u \pmod p \quad \prod_{i=1}^3 x_i\equiv u \pmod p \quad \prod_{i=1}^2 x_i\equiv u \pmod p$$

Hence we get

$$\sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}\sum_{\substack{\prod_{i=1}^{3} x_i \equiv u \pmod p}} 1 = (p-1)^2 - 3(p-3) - 3 = p^2 - 5p + 7$$

which yields

$$\sum_{x_1=2}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}\sum_{x_4=2}^{p-1}\sum_{\substack{\prod_{i=1}^{4} x_i \equiv u \pmod p}} 1 = (p-1)^3 - 4(p^2-5p+7) - 6(p-3) - 4$$

$$= p^3 - 7p^2 + 17p - 15.$$

Thus from (3.26) we deduce that

$$\sum_{x_1=2}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}\sum_{x_4=2}^{p-1}\sum_{y_1=2}^{p-1}\sum_{y_2=2}^{p-1}\sum_{y_3=2}^{p-1}\sum_{y_4=2}^{p-1}\sum_{\substack{\prod_{i=1}^{4} x_i \equiv \prod_{i=1}^{4} y_i \pmod p}} \chi_0(x_1x_2x_3x_4 - 1)$$

$$= \sum_{u=2}^{p-1}\left(\sum_{x_1=2}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}\sum_{x_4=2}^{p-1}\sum_{\substack{\prod_{i=1}^{4} x_i \equiv u \pmod p}} 1\right)^2$$

$$= (p-2)(p^3 - 7p^2 + 17p - 15)^2$$

$$= p^7 - 16p^6 + 111p^5 - 434p^4 + 1035p^3 - 1508p^2 + 1245p - 450.$$

This completes the proof of the lemma. ■

The proof of the next lemma is very similar to [42, Lemma 2.1].

Lemma 3.7. *Let p be an odd prime and χ be any Dirichlet character mod p. Then we have the identity*

$$\sum_{m=1}^{p-1}\left|\sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{x_4=1}^{p-1}\chi(\prod_{i=1}^{4} x_i)e\left(\frac{\sum_{i=1}^{4} x_i + m\prod_{i=1}^{4}\overline{x_i}}{p}\right)\right|^2$$

$$= \begin{cases} p^5 - 2p^4 - p^3 - p^2 - p, & \text{if } \chi \neq \chi_0; \\ p^5 - p^4 - p^3 - p^2 - p - 1, & \text{if } \chi = \chi_0. \end{cases}$$

Proof. We first note the following identity

$$\sum_{m=0}^{p-1} e\left(\frac{nm}{p}\right) = \begin{cases} p, & \text{if } p|n; \\ 0, & \text{if } p \nmid n. \end{cases}$$

Using the above identity, we have

$$\begin{aligned}
&\sum_{m=0}^{p-1} \left| \sum_X \chi(\prod_{i=1}^4 x_i) e\left(\frac{\sum_{i=1}^4 x_i + m\prod_{i=1}^4 \overline{x_i}}{p}\right)\right|^2 \\
&= \sum_X \sum_Y \chi(\prod_{i=1}^4 x_i\overline{y_i}) \sum_{m=0}^{p-1} e\left(\frac{\sum_{i=1}^4 x_i - \sum_{i=1}^4 y_i + m(\prod_{i=1}^4 \overline{x_i} - \prod_{i=1}^4 \overline{y_i})}{p}\right) \\
&= \sum_X \sum_Y \chi(\prod_{i=1}^4 x_i) e\left(\frac{\sum_{i=1}^4 y_i(x_i-1)}{p}\right) \times \sum_{m=0}^{p-1} e\left(\frac{m\prod_{i=1}^4 \overline{y_i}(\prod_{i=1}^4 \overline{x_i} - 1)}{p}\right) \\
&= p \sum_{\substack{X \\ \prod_{i=1}^4 x_i \equiv 1 \pmod p}} \chi(\prod_{i=1}^4 x_i) \sum_Y e\left(\frac{\sum_{i=1}^4 y_i(x_i-1)}{p}\right) \\
&= p\sum_Y 1 + 4p \sum_{\substack{x_1=2}}^{p-1} \sum_{x_2=2}^{p-1} \sum_{x_3=2}^{p-1} \sum_Y e\left(\frac{\sum_{i=1}^3 y_i(x_i-1)}{p}\right) \\
&\qquad \prod_{i=1}^3 x_i \equiv 1 \pmod p \\
&+6p \sum_{x_1=2}^{p-1} \sum_Y e\left(\frac{y_1(x_1-1) + y_2(\overline{x_1}-1)}{p}\right) \\
&+p \sum_{\substack{x_1=2}}^{p-1} \sum_{x_2=2}^{p-1} \sum_{x_3=2}^{p-1} \sum_{x_4=2}^{p-1} \sum_Y e\left(\frac{\sum_{i=1}^4 y_i(x_i-1)}{p}\right). \qquad (3.27) \\
&\qquad \prod_{i=1}^4 x_i \equiv 1 \pmod p
\end{aligned}$$

We obtain (3.27) by dividing the set of solutions of the congruence $\prod_{i=1}^4 x_i \equiv 1 \pmod p$ into four cases: all x_i's are equal to 1, exactly one of the x_i's is equal to 1, exactly two of x_i's are equal to 1, and none of x_i's is equal to 1. We now evaluate

the above three sums of (3.27). Firstly, we have

$$\sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}\sum_{Y} e\left(\frac{\sum_{i=1}^{3} y_i(x_i-1)}{p}\right) \tag{3.28}$$
$$\prod_{i=1}^{3} x_i \equiv 1 \pmod p$$

$$= -(p-1)\sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1} 1$$
$$\prod_{i=1}^{3} x_i \equiv 1 \pmod p$$

$$= -(p-1)\left[\sum_{\substack{x_1=1}}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1} 1 - 3\sum_{x_1=2}^{p-1} 1 - 1\right]$$
$$\prod_{i=1}^{3} x_i \equiv 1 \pmod p$$

$$= -(p-1)[(p-1)^2 - 3(p-2) - 1]$$

$$= -(p^3 - 6p^2 + 11p - 6). \tag{3.29}$$

Similarly, we get

$$\sum_{x_1=2}^{p-1}\sum_{Y} e\left(\frac{y_1(x_1-1)+y_2(\overline{x_1}-1)}{p}\right) = (p-1)^2(p-2)$$
$$= p^3 - 4p^2 + 5p - 2. \tag{3.30}$$

Finally,

$$\sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}\sum_{x_4=2}^{p-1}\sum_{Y} e\left(\frac{\sum_{i=1}^{4} y_i(x_i-1)}{p}\right)$$
$$\prod_{i=1}^{4} x_i \equiv 1 \pmod p$$

$$= \sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1}\sum_{x_4=2}^{p-1} 1$$
$$\prod_{i=1}^{4} x_i \equiv 1 \pmod p$$

$$= \sum_{\substack{x_1=1}}^{p-1}\sum_{x_2=1}^{p-1}\sum_{x_3=1}^{p-1}\sum_{x_4=1}^{p-1} 1 - 4\sum_{\substack{x_1=2}}^{p-1}\sum_{x_2=2}^{p-1}\sum_{x_3=2}^{p-1} 1 - 6\sum_{x_1=2}^{p-1} 1 - 1$$
$$\prod_{i=1}^{4} x_i \equiv 1 \pmod p \qquad \prod_{i=1}^{3} x_i \equiv 1 \pmod p$$

$$= (p-1)^3 - 4[(p-1)^2 - 3(p-2) - 1] - 6(p-2) - 1$$
$$= p^3 - 7p^2 + 17p - 14. \tag{3.31}$$

Again, from the properties of Gauss sums we have

$$\left|\sum_X \chi(x_1x_2x_3x_4)e\left(\frac{x_1+x_2+x_3+x_4}{p}\right)\right|^2 = \begin{cases} p^4, & \text{if } \chi \neq \chi_0; \\ 1, & \text{if } \chi = \chi_0. \end{cases} \tag{3.32}$$

Now combining (3.27), (3.28), (3.30), (3.31) and (3.32), we readily obtain the required identity. ■

Lemma 3.8. *Let p be an odd prime and χ be any character mod p. Then for primitive character χ_1 mod p, we have the identity*

$$\left|\sum_{m=1}^{p-1}\chi_1(m)\left|\sum_X \chi(x_1x_2x_3x_4)e\left(\frac{x_1+x_2+x_3+x_4+m\overline{x_1x_2x_3x_4}}{p}\right)\right|^2\right|^2$$
$$= p^5\left|\sum_X \chi(x_1x_2x_3x_4)\overline{\chi_1}((\overline{x_1x_2x_3x_4}-1)(x_1-1)(x_2-1)(x_3-1)(x_4-1))\right|^2.$$

Proof. The proof proceeds along similar lines to the proof of [42, Lemma 2.3] so we omit the details for reasons of brevity. ■

3.5 Proof of the main result

We now have all the ingredients to prove our main theorem.

Proof of Theorem 3.1. From the orthogonality property of characters mod p we have

$$\sum_{\chi \bmod p}\sum_{\chi_1 \bmod p}\left|\sum_{m=1}^{p-1}\chi_1(m)\left|\sum_X \chi(\prod_{i=1}^4 x_i)e\left(\frac{\sum_{i=1}^4 x_i + m\prod_{i=1}^4 \overline{x_i}}{p}\right)\right|^2\right|^2$$

$$= (p-1)\sum_{m=1}^{p-1}\sum_{\chi \bmod p}\left|\sum_{X}\chi(\prod_{i=1}^{4}x_i)e\left(\frac{\sum_{i=1}^{4}x_i + m\prod_{i=1}^{4}\overline{x_i}}{p}\right)\right|^4. \tag{3.33}$$

Also we have

$$\begin{aligned}
&\sum_{\chi \bmod p}\sum_{\chi_1 \bmod p}\left|\sum_{m=1}^{p-1}\chi_1(m)\left|\sum_{X}\chi(\prod_{i=1}^{4}x_i)e\left(\frac{\sum_{i=1}^{4}x_i + m\prod_{i=1}^{4}\overline{x_i}}{p}\right)\right|^2\right|^2\\
&= \sum_{\chi \bmod p}\sum_{\substack{\chi_1 \bmod p\\ \chi_1\neq\chi_0}}\left|\sum_{m=1}^{p-1}\chi_1(m)\left|\sum_{X}\chi(\prod_{i=1}^{4}x_i)e\left(\frac{\sum_{i=1}^{4}x_i + m\prod_{i=1}^{4}\overline{x_i}}{p}\right)\right|^2\right|^2\\
&\quad+\sum_{\chi \bmod p}\left|\sum_{m=1}^{p-1}\left|\sum_{X}\chi(\prod_{i=1}^{4}x_i)e\left(\frac{\sum_{i=1}^{4}x_i + m\prod_{i=1}^{4}\overline{x_i}}{p}\right)\right|^2\right|^2.
\end{aligned} \tag{3.34}$$

Using Lemma 3.7 we obtain

$$\begin{aligned}
&\sum_{\chi \bmod p}\left|\sum_{m=1}^{p-1}\left|\sum_{X}\chi(\prod_{i=1}^{4}x_i)e\left(\frac{\sum_{i=1}^{4}x_i + m\prod_{i=1}^{4}\overline{x_i}}{p}\right)\right|^2\right|^2\\
&= (p-2)(p^5-2p^4-p^3-p^2-p)^2 + (p^5-p^4-p^3-p^2-p-1)^2\\
&= (p-1)(p^{10}+O(p^9)).
\end{aligned} \tag{3.35}$$

Now using Lemmas 3.5, 3.6 and 3.8 we have

$$\begin{aligned}
&\sum_{\chi \bmod p}\sum_{\substack{\chi_1 \bmod p\\ \chi_1\neq\chi_0}}\left|\sum_{m=1}^{p-1}\chi_1(m)\left|\sum_{X}\chi(\prod_{i=1}^{4}x_i)e\left(\frac{\sum_{i=1}^{4}x_i + m\prod_{i=1}^{4}\overline{x_i}}{p}\right)\right|^2\right|^2\\
&= p^5\sum_{\chi \bmod p}\sum_{\substack{\chi_1 \bmod p\\ \chi_1\neq\chi_0}}\left|\sum_{X}\chi(\prod_{i=1}^{4}x_i)\overline{\chi_1}((\prod_{i=1}^{4}\overline{x_i}-1)\prod_{i=1}^{4}(x_i-1))\right|^2\\
&= p^5\sum_{\chi \bmod p}\sum_{\chi_1 \bmod p}\left|\sum_{X}\chi(\prod_{i=1}^{4}x_i)\overline{\chi_1}((\prod_{i=1}^{4}\overline{x_i}-1)\prod_{i=1}^{4}(x_i-1))\right|^2
\end{aligned}$$

$$
\begin{aligned}
&-p^5 \sum_{\chi \bmod p} \left| \sum_X \chi(\prod_{i=1}^4 x_i)\overline{\chi_0}((\prod_{i=1}^4 \overline{x_i} - 1)\prod_{i=1}^4 (x_i - 1)) \right|^2 \\
&= p^5(p-1)^2 \sum_X \sum_Y \chi_0((\prod_{i=1}^4 \overline{x_i} - 1)\prod_{i=1}^4 (x_i - 1)) \\
&\qquad \prod_{i=1}^4 x_i \equiv \prod_{i=1}^4 y_i \pmod p \\
&\qquad \prod_{i=1}^4 (x_i - 1) \equiv \prod_{i=1}^4 (y_i - 1) \pmod p \\
&-p^5(p-1) \sum_{x_1=2}^{p-1} \sum_{x_2=2}^{p-1} \sum_{x_3=2}^{p-1} \sum_{x_4=2}^{p-1} \sum_{y_1=2}^{p-1} \sum_{y_2=2}^{p-1} \sum_{y_3=2}^{p-1} \sum_{y_4=2}^{p-1} \chi_0(\prod_{i=1}^4 x_i - 1) \\
&\qquad \prod_{i=1}^4 x_i \equiv \prod_{i=1}^4 y_i \pmod p \\
&= p^5(p-1)^2(p^6 - 15p^5 + 97p^4 + O(p^3)) \\
&-p^5(p-1)(p^7 - 16p^6 + 111p^5 - 434p^4 + 1035p^3 - 1508p^2 + 1245p - 450) \\
&= (p-1)(p^{10} + O(p^9)). \qquad (3.36)
\end{aligned}
$$

Hence from (3.34), (3.35) and (3.36) we obtain

$$
\begin{aligned}
&\sum_{\chi \bmod p} \sum_{\chi_1 \bmod p} \left| \sum_{m=1}^{p-1} \chi_1(m) \left| \sum_X \chi(\prod_{i=1}^4 x_i) e\left(\frac{\sum_{i=1}^4 x_i + m\prod_{i=1}^4 \overline{x_i}}{p} \right) \right|^2 \right|^2 \\
&= (p-1)(p^{10} + O(p^9)) + (p-1)(p^{10} + O(p^9)) \\
&= (p-1)(2p^{10} + O(p^9)). \qquad (3.37)
\end{aligned}
$$

Using (3.33) and (3.37) we complete the proof of our main theorem. ■

4

Generalized quadratic Gauss sums weighted by L-functions

4.1 Introduction and statement of the result

Let $q \geq 2$ be an integer, and let χ be a Dirichlet character modulo q. For $n \in \mathbb{Z}$, we recall the *generalized quadratic Gauss sum* $G(n, \chi; q)$ which is defined as

$$G(n, \chi; q) = \sum_{a=1}^{q} \chi(a) e\left(\frac{na^2}{q}\right),$$

[1]The contents of this chapter have been accepted for publication in the *Asian Journal of Mathematics* (2020).

where $e(y) = e^{2\pi iy}$. This sum generalizes the classical *quadratic Gauss sum* $G(n;q)$, which is defined as

$$G(n;q) = \sum_{a=1}^{q} e\left(\frac{na^2}{q}\right).$$

The properties of $G(n,\chi;q)$ have been studied for a long time. The values of $G(n,\chi;q)$ behave irregularly as χ varies. From a result of Cochrane and Zheng [11], one can find an upper bound of $|G(n,\chi;q)|$ for any positive integer n with $\gcd(n,q) = 1$. Let p be an odd prime and $L(s,\chi)$ denote the Dirichlet L-function corresponding to the character $\chi \mod p$. Let χ_0 denote the principal character modulo p. For a general integer $m \geq 3$, whether there exists an asymptotic formula for

$$\sum_{\chi \bmod p} |G(n,\chi;p)|^{2m} \text{ and } \sum_{\chi \neq \chi_0} |G(n,\chi;p)|^{2m} \cdot |L(1,\chi)|$$

is an unsolved problem. In [40], Zhang conjectured the following.

Conjecture 4.1. *For all positive integers m,*

$$\sum_{\chi \neq \chi_0} |G(n,\chi;p)|^{2m} \cdot |L(1,\chi)| \sim C \sum_{\chi \pmod p} |G(n,\chi;p)|^{2m}, \qquad p \to +\infty,$$

where

$$C = \prod_p \left[1 + \frac{\binom{2}{1}^2}{4^2.p^2} + \frac{\binom{4}{2}^2}{4^4.p^4} + \cdots + \frac{\binom{2m}{m}^2}{4^{2m}.p^{2m}} + \cdots\right] \tag{4.1}$$

is a constant and $\prod_p$ denotes the product over all primes.

For an analogous study on central value of moments of twisted L-functions, see [4]. For a fairly general family of L-functions, V. Blomer, É. Fouvry, E. Kowalski, P. Michel, D. Milićević and W. Sawin surveyed the known consequences of the existence of the asymptotic formulas with power saving error term for the twisted first and

second moments of the central value of the family. Their works also contribute to many arithmetic consequences regarding L-functions. For further study related to moments of twisted L-functions see [3, 5, 39].

Zhang [40] showed that $G(n, \chi; p)$ enjoys many good weighted mean value properties. He used estimates for character sums and analytic methods to study the second, fourth and sixth order moments of generalized quadratic Gauss sums weighted by L-functions. To be specific, he proved that for any integer n with $\gcd(n, p) = 1$,

$$\sum_{\chi \neq \chi_0} |G(n, \chi; p)|^2 \cdot |L(1, \chi)| = C \cdot p^2 + O(p^{3/2} \cdot \ln^2 p)$$

and

$$\sum_{\chi \neq \chi_0} |G(n, \chi; p)|^4 \cdot |L(1, \chi)| = 3 \cdot C \cdot p^3 + O(p^{5/2} \cdot \ln^2 p),$$

where C is given by (4.1). He also found the following asymptotic formula for the $6th$ order moment of the generalized quadratic Gauss sums. He proved that, for an odd prime $p \equiv 3 \pmod 4$ and for any fixed positive integer n with $\gcd(n, p) = 1$,

$$\sum_{\chi \neq \chi_0} |G(n, \chi; p)|^6 \cdot |L(1, \chi)| = 10 \cdot C \cdot p^4 + O(p^{7/2} \cdot \ln^2 p).$$

Finding asymptotic formulas for the $6th$ order moment in case of $p \equiv 1 \pmod 4$ and for the higher order moments seem to be more difficult. To find asymptotic formulas for the higher order moments, one needs to estimate more complicated character sums, and the ideas used in [40] are not sufficient to estimate such character sums. In this chapter, we employ certain ideas from algebraic geometry to estimate the following three character sums.

Theorem 4.2. *Let p be an odd prime, and let $a \in \mathbb{F}_p \setminus \{0, \pm 1\}$. Then we have*

$$\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}\left(\frac{b^2-a^2c^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{d^2-c^2}{p}\right)\left(\frac{d^2-1}{p}\right) = O(p^{3/2}).$$

The proof of Theorem 4.2 does not hold for $a = \pm 1$. In the following theorem we find an asymptotic formula for the above sum in case of $a = \pm 1$.

Theorem 4.3. *Let p be an odd prime. We have*

$$\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}\left(\frac{b^2-c^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{d^2-c^2}{p}\right)\left(\frac{d^2-1}{p}\right) = 3p^2 + O(p^{3/2}).$$

Theorem 4.4. *Let p be an odd prime. For $a \in \mathbb{F}_p^{\times}$, we have*

$$\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{b^2-a^2c^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{c^2-1}{p}\right) = O(p).$$

We use the above three estimates to find an asymptotic formula for the $6th$ order moment in case of $p \equiv 1 \pmod 4$ and an asymptotic formula for the $8th$ order moment of generalized quadratic Gauss sums weighted by L-functions. To be specific, we prove the following two main theorems.

Theorem 4.5. *Let p be an odd prime satisfying $p \equiv 1 \pmod 4$. For any integer n with $\gcd(n, p) = 1$, we have the asymptotic formula*

$$\sum_{\chi \neq \chi_0} |G(n, \chi; p)|^6 \cdot |L(1, \chi)| = 10 \cdot C \cdot p^4 + O(p^{7/2} \cdot \ln p),$$

where C is as given in (4.1).

Theorem 4.6. *Let p be an odd prime. For any integer n with $\gcd(n, p) = 1$, we*

have the asymptotic formula

$$\sum_{\chi \neq \chi_0} |G(n,\chi;p)|^8 \cdot |L(1,\chi)| = 35 \cdot C \cdot p^5 + O(p^{9/2} \cdot \ln p),$$

where C is as given in (4.1).

Combining the results proved in [18, 40], it readily follows that Conjecture 4.1 is true when $m = 1, 2$. He and Liao [18, Theorem 2] evaluated the sum $\sum_{\chi \bmod p} |G(n,\chi;p)|^6$ for any integer n with $\gcd(n,p) = 1$. They proved that

$$\sum_{\chi \bmod p} |G(n,\chi;p)|^6 = \begin{cases} (p-1)(10p^3 - 25p^2 - 16p - 1) + (p\sqrt{p}(p-1)N \\ +18p^2\sqrt{p} - 12p\sqrt{p} - 6\sqrt{p})\left(\frac{n}{p}\right), & \text{if } p \equiv 1 \pmod 4; \\ (p-1)(10p^3 - 25p^2 - 4p - 1), & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where

$$N = \sum_{a=2}^{p-2} \sum_{c=1}^{p-1} \left(\frac{a^2 - c^2}{p}\right)\left(\frac{c^2 - 1}{p}\right)\left(\frac{a^2 - 1}{p}\right). \tag{4.2}$$

In this chapter we find an asymptotic formula for the character sum N and obtain an improved estimate of He and Liao's result as given below.

Theorem 4.7. *Let p be an odd prime and n be any integer with $\gcd(n,d) = 1$. Then we have*

$$\sum_{\chi \bmod p} |G(n,\chi;p)|^6 = \begin{cases} 10p^4 + O(p^{7/2}), & \text{if } p \equiv 1 \pmod 4; \\ (p-1)(10p^3 - 25p^2 - 4p - 1), & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

From the works of He and Liao [18] and Zhang [40], it follows that Conjecture 4.1 is true when $m = 3$ and $p \equiv 3 \pmod 4$. Using Theorem 4.5 and Theorem 4.7 we now readily find that Conjecture 4.1 is also true when $m = 3$ and $p \equiv 1 \pmod 4$.

He and Liao [18, Theorem 3] also evaluated the sum $\sum_{\chi \bmod p} |G(n,\chi;p)|^8$ for any integer n with $\gcd(n,p)=1$. They proved that

$$\sum_{\chi \bmod p} |G(n,\chi;p)|^8$$
$$= \begin{cases} (p-1)(34p^4-99p^3-65p^2-29p-1) \\ +(56p^3\sqrt{p}+8p^2\sqrt{p}-56p\sqrt{p}-8\sqrt{p}+8p^2\sqrt{p}(p-1)N)\left(\frac{n}{p}\right) \\ +p^2(p-1)T, & \text{if } p\equiv 1 \pmod 4; \\ (p-1)(34p^4-99p^3+7p^2-5p-1)+p^2(p-1)T, & \text{if } p\equiv 3 \pmod 4, \end{cases}$$

where N is the same as (4.2) and

$$T=\sum_{a=2}^{p-2}\sum_{b=1}^{p-1}\sum_{d=1}^{p-1}\left(\frac{a^2-b^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{a^2-d^2}{p}\right)\left(\frac{d^2-1}{p}\right). \tag{4.3}$$

In this chapter we find an asymptotic formula for the character sum T and obtain an improved estimate of He and Liao's result as given below.

Theorem 4.8. *Let p be an odd prime and n be any integer with $\gcd(n,d)=1$. Then we have*

$$\sum_{\chi \bmod p} |G(n,\chi;p)|^8 = 35p^5+O(p^{9/2}).$$

Combining Theorem 4.6 and Theorem 4.8 we find that Conjecture 4.1 is also true when $m=4$.

4.2 Proof of Theorems 4.2, 4.3, and 4.4

In this section we prove Theorems 4.2, 4.3, and 4.4. These three results play crucial role in the proof of our main results. Our proofs rely on certain techniques from algebraic geometry. Throughout this section, we set $\rho(t):=\left(\frac{t}{p}\right)$, where $\left(\frac{\bullet}{p}\right)$

is the Legendre symbol.

Proof of Theorem 4.2. Let

$$S := \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1} \rho(b^2 - a^2c^2)\rho(b^2-1)\rho(d^2-c^2)\rho(d^2-1),$$

where $a \in \mathbb{F}_p \setminus \{0, \pm 1\}$. We can rewrite the above sum as

$$\begin{aligned} S &= \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1} \rho(b - a^2c^2)\rho(b-1)\rho(d^2-c^2)\rho(d^2-1)\#\{x : x^2 = b\} \\ &= \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1} \rho(b - a^2c^2)\rho(b-1)\rho(d^2-c^2)\rho(d^2-1)(1+\rho(b)) \\ &= S_1 + S_2, \end{aligned}$$

where

$$S_1 = \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1} \rho(b - a^2c^2)\rho(b-1)\rho(d^2-c^2)\rho(d^2-1)$$

and

$$S_2 = \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1} \rho(b - a^2c^2)\rho(b-1)\rho(b)\rho(d^2-c^2)\rho(d^2-1).$$

Now

$$\begin{aligned} S_1 &= \sum_{c=1}^{p-1}\sum_{d=1}^{p-1} \rho(d^2-c^2)\rho(d^2-1) \sum_{b=1}^{p-1} \rho(b - a^2c^2)\rho(b-1) \\ &= \sum_{c=1}^{p-1}\sum_{d=1}^{p-1} \rho(d^2-c^2)\rho(d^2-1) \sum_{b=1}^{p} \rho(b - a^2c^2)\rho(b-1) \\ &\qquad - \sum_{c=1}^{p-1}\sum_{d=1}^{p-1} \rho(d^2-c^2)\rho(d^2-1) \end{aligned}$$

$$= \sum_{c=1}^{p-1}\sum_{d=1}^{p-1} \rho(d^2-c^2)\rho(d^2-1) \sum_{b=1}^{p} \rho(b-a^2c^2)\rho(b-1) + O(p^{3/2}).$$

The inner sum is -1 if $ac \neq \pm 1$ and $p-1$ if $ac = \pm 1$, and hence

$$S_1 = -\sum_{c=1, c\neq \pm a^{-1}}^{p-1} \sum_{d=1}^{p-1} \rho(d^2-c^2)\rho(d^2-1) + 2(p-1)\sum_{d=1}^{p-1} \rho(d^2-a^{-2})\rho(d^2-1) + O(p^{3/2}).$$

Both the sums are $O(p^{3/2})$ because neither $(d^2-c^2)(d^2-1)$ nor $(d^2-a^{-2})(d^2-1)$ is a perfect square in $\overline{\mathbb{F}_p}[c,d]$. So we obtain

$$S = S_2 + O(p^{3/2}).$$

Now we repeat the same argument with c and d on S_2, and deduce that

$$S = S' + O(p^{3/2}),$$

where

$$\begin{aligned} S' &= \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1} \rho(b-a^2c)\rho(b-1)\rho(b)\rho(d-c)\rho(d-1)\rho(d)\rho(c) \\ &= \sum_{c=1}^{p-1} \rho(c) \left(\sum_{b=1}^{p-1} \rho(b-a^2c)\rho(b-1)\rho(b)\right)\left(\sum_{d=1}^{p-1} \rho(d-c)\rho(d-1)\rho(d)\right) \\ &= \sum_{c=1}^{p-1} \rho(c)\phi(a^2c)\phi(c), \end{aligned}$$

considering $\phi(t) = \sum_{b=1}^{p-1} \rho(b-t)\rho(b-1)\rho(b)$. Here $\phi(t)$ is the trace function of the self-dual, rank 2, irreducible sheaf $\mathcal{F}$, which is a non-trivial cohomology sheaf of the Legendre family of elliptic curve

$$y^2 = x(x-1)(x-t)$$

and $\rho(c)$ is the trace function of the rank 1 Kummer sheaf $\mathcal{L}_\rho$, associated to the quadratic character ρ. Here $\mathcal{F}$ is not isomorphic to a twist of $\mathcal{G} := \alpha^*\mathcal{F}$, where the map α is the multiplicative translation by a^2 and $a \in \mathbb{F}_p \setminus \{0, \pm 1\}$. Both $\mathcal{F}$ and $\mathcal{G}$ are of weight 1 and we consider trace functions of weight less than or equal to 0. Hence we normalise both trace functions of $\mathcal{F}$ and $\mathcal{G}$ dividing by $\sqrt{p}$. Here $\mathcal{G}$ and $\mathcal{F} \otimes \mathcal{L}_\rho$ both are geometrically irreducible. Here $\mathcal{F} \otimes \mathcal{L}_\rho$ is geometrically irreducible because tensoring with one dimensional sheaf preserves geometric irreducibility. In any odd characteristic $\mathcal{F} \otimes \mathcal{L}_\rho$ has non-trivial (in fact unipotent) local monodromy at 1, but is lisse at $1/a^2$, whereas the multiplicative translate $\mathcal{G}$ has non-trivial (in fact unipotent) local monodromy at $1/a^2$, but is lisse at 1. Note that $\mathcal{G}$ is a self-dual sheaf. Hence $\mathcal{F} \otimes \mathcal{L}_\rho$ is not geometrically isomorphic to the dual of $\mathcal{G}$. Hence from Theorem 1.1 we find that

$$\frac{1}{p}\sum_{c=1}^{p-1}\rho(c)\frac{\phi(a^2c)}{\sqrt{p}}\frac{\phi(c)}{\sqrt{p}} = O\left(\frac{(C(\mathcal{F}))^2(C(\mathcal{G}))^2(C(\mathcal{L}_\rho))^2}{\sqrt{p}}\right),$$

where $C(\mathcal{F})$, $C(\mathcal{G})$ and $C(\mathcal{L}_\rho)$ are the conductors of the sheaves. We have $C(\mathcal{L}_\rho) = O(1)$. Now $\mathcal{F}$ is of rank 2 and is at most tamely ramified at 0, 1 and ∞ and lisse elsewhere, so all the $\mathrm{Swan}_x(\mathcal{F})$ are zero and the conductor is bounded by 5. So we have $C(\mathcal{F}) = C(\mathcal{G}) = O(1)$, which implies

$$\sum_{c=1}^{p-1}\rho(c)\phi(a^2c)\phi(c) = p^2 O\left(\frac{C(\mathcal{F})C(\mathcal{G})C(\mathcal{L}_\rho)}{\sqrt{p}}\right) = O\left(p^{3/2}\right).$$

Finally, applying the estimate for S' in S, we complete the proof. ∎

Proof of Theorem 4.3. We observe that

$$\begin{aligned}&\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}\left(\frac{b^2-c^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{d^2-c^2}{p}\right)\left(\frac{d^2-1}{p}\right)\\ &= 2(p-3)^2 + T, \end{aligned} \tag{4.4}$$

where

$$T = \sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\left(\frac{b^2-c^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{d^2-c^2}{p}\right)\left(\frac{d^2-1}{p}\right)$$

is the same as given in (4.3). Proceeding similarly as shown in the proof of Theorem 4.2 we write

$$\begin{aligned} T &= \sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\rho(b^2-c^2)\rho(b^2-1)\rho(d^2-c^2)\rho(d^2-1) \\ &= \sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\rho(b-c^2)\rho(b-1)\rho(d^2-c^2)\rho(d^2-1)(1+\rho(b)) \\ &= T_1 + T_2, \end{aligned}$$

where

$$T_1 = \sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\rho(b-c^2)\rho(b-1)\rho(d^2-c^2)\rho(d^2-1)$$

and

$$T_2 = \sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\rho(b-c^2)\rho(b-1)\rho(b)\rho(d^2-c^2)\rho(d^2-1).$$

We find that

$$\begin{aligned} T_1 &= \sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\rho(d^2-c^2)\rho(d^2-1)\sum_{b=1}^{p-1}\rho(b-c^2)\rho(b-1) \\ &= \sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\rho(d^2-c^2)\rho(d^2-1)\sum_{b=1}^{p}\rho(b-c^2)\rho(b-1) \\ &\qquad - \sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\rho(d^2-c^2)\rho(d^2-1) \end{aligned}$$

$$= -2\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\rho(d^2-c^2)\rho(d^2-1)$$
$$= O(p^{3/2}).$$

Now we use the same argument on T_2 for d, which gives

$$T_2 = \sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\rho(b-c^2)\rho(b-1)\rho(b)\rho(d-c^2)\rho(d-1)(1+\rho(d))$$
$$= T_2' + T_2'',$$

where

$$T_2' = \sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\rho(b-c^2)\rho(b-1)\rho(b)\rho(d-c^2)\rho(d-1)$$

and

$$T_2'' = \sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\rho(b-c^2)\rho(b-1)\rho(b)\rho(d-c^2)\rho(d-1)\rho(d).$$

We first find that

$$T_2' = \sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\rho(b-c^2)\rho(b-1)\rho(b)\sum_{d=1}^{p-1}\rho(d-c^2)\rho(d-1)$$
$$= \sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\rho(b-c^2)\rho(b-1)\rho(b)\sum_{d=1}^{p}\rho(d-c^2)\rho(d-1)$$
$$- \sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\rho(b-c^2)\rho(b-1)\rho(b)$$
$$= -2\sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\rho(b-c^2)\rho(b-1)\rho(b)$$
$$= O(p^{3/2}).$$

Now

$$\begin{aligned}
T_2'' &= \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}\rho(b-c^2)\rho(b-1)\rho(b)\rho(d-c^2)\rho(d-1)\rho(d) - 2\sum_{b=2}^{p-1}\sum_{d=2}^{p-1}\rho(b)\rho(d)\\
&= \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}\rho(b-c)\rho(b-1)\rho(b)\rho(d-c)\rho(d-1)\rho(d)(1+\rho(c)) + O(1)\\
&= \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}\rho(b-c)\rho(b-1)\rho(b)\rho(d-c)\rho(d-1)\rho(d)\rho(c)\\
&\qquad + \sum_{b=1}^{p-1}\sum_{d=1}^{p-1}\rho(b-1)\rho(b)\rho(d-1)\rho(d)\sum_{c=1}^{p-1}\rho(c-b)\rho(c-d) + O(1)\\
&= \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}\rho(b-c)\rho(b-1)\rho(b)\rho(d-c)\rho(d-1)\rho(d)\rho(c)\\
&\qquad + (p-1)(p-2) + O(p).
\end{aligned}$$

Hence we have

$$\begin{aligned}
T &= T_1 + T_2\\
&= O(p^{3/2}) + T_2' + T_2''\\
&= T' + (p-1)(p-2) + O(p^{3/2}),
\end{aligned}$$

where

$$\begin{aligned}
T' &= \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}\rho(b-c)\rho(b-1)\rho(b)\rho(d-c)\rho(d-1)\rho(d)\rho(c)\\
&= \sum_{c=1}^{p-1}\rho(c)\left(\sum_{b=1}^{p-1}\rho(b-c)\rho(b-1)\rho(b)\right)\left(\sum_{d=1}^{p-1}\rho(d-c)\rho(d-1)\rho(d)\right)\\
&= \sum_{c=1}^{p-1}\rho(c)\phi^2(c).
\end{aligned}$$

Here $\phi(t) = \sum_{b=1}^{p-1}\rho(b)\rho(b-1)\rho(b-t)$. Note that $\phi(t)$ and $\rho(c)$ are the trace functions of the cohomology sheaf $\mathcal{F}$ and $\mathcal{L}_\rho$ as defined in the proof of Theorem 4.2. We

normalise the trace function of $\mathcal{F}$ dividing by $\sqrt{p}$. Note that $\mathcal{F}\otimes\mathcal{L}_\rho$ is geometrically irreducible, as tensoring with one dimensional sheaf preserves geometric irreducibility. Also $\mathcal{F}\otimes\mathcal{L}_\rho$ is not geometrically isomorphic to the dual of $\mathcal{F}$, which can be checked using the local monodromy representation at 0. For the Legendre family, it is unipotent as the reduction is semi-stable, but for tensoring with Kummer sheaf $\mathcal{L}_\rho$, it is non-unipotent. Hence from Theorem 1.1 we obtain

$$\frac{1}{p}\sum_{c=1}^{p-1}\rho(c)\frac{\phi^2(c)}{p} = O\left(\frac{(C(\mathcal{F}))^4(C(\mathcal{L}_\rho)^2}{\sqrt{p}}\right),$$

where $C(\mathcal{F}) = C(\mathcal{L}_\rho) = O(1)$, which finally implies

$$\sum_{c=1}^{p-1}\rho(c)\phi^2(c) = O(p^{3/2}).$$

Replacing the estimate for T' in T we have

$$T = p^2 + O(p^{3/2}). \tag{4.5}$$

Combining (4.4) and (4.5) we complete the proof. ■

Proof of Theorem 4.4. We consider

$$\begin{aligned} R &= \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\rho(b^2-a^2c^2)\rho(b^2-1)\rho(c^2-1)\\ &= \sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\rho(b-a^2c^2)\rho(b-1)\rho(c^2-1)(1+\rho(b))\\ &= R_1 + R_2, \end{aligned}$$

where

$$R_1 = \sum_{b=1}^{p-1}\sum_{c=1}^{p-1} \rho(b-a^2c^2)\rho(b-1)\rho(c^2-1)$$

and

$$R_2 = \sum_{b=1}^{p-1}\sum_{c=1}^{p-1} \rho(b-a^2c^2)\rho(b-1)\rho(b)\rho(c^2-1).$$

We write

$$\begin{aligned} R_1 &= \sum_{c=1}^{p-1}\rho(c^2-1)\sum_{b=1}^{p-1}\rho(b-a^2c^2)\rho(b-1) \\ &= \sum_{c=1}^{p-1}\rho(c^2-1)\sum_{b=1}^{p}\rho(b-a^2c^2)\rho(b-1) - \sum_{c=1}^{p-1}\rho(c^2-1) \\ &= \sum_{c=1}^{p-1}\rho(c^2-1)\sum_{b=1}^{p}\rho(b-a^2c^2)\rho(b-1) + O(p). \end{aligned}$$

Then inner sum is -1 if $ac \neq \pm 1$ and $p-1$ if $ac = \pm 1$, hence we have

$$R_1 = 2(p-1)\rho(a^{-2}-1) - \sum_{c=1, c\neq \pm a^{-1}}^{p-1} \rho(c^2-1) + O(p),$$

which implies $R_1 = O(p)$. So we get

$$R = R_2 + O(p).$$

Repeating the same argument with c on R_2 we obtain

$$R = R' + O(p),$$

where

$$R' = \sum_{c=1}^{p-1} \rho(c-1)\rho(c) \sum_{b=1}^{p-1} \rho(b-a^2c)\rho(b-1)\rho(b)$$
$$= \sum_{c=1}^{p-1} \rho(c^2-c)\phi(a^2c),$$

where $\phi(t) = \sum_{b=1}^{p-1} \rho(b-t)\rho(b-1)\rho(b)$. Here we are working with the trace function $\phi(a^2c)$ of $\mathcal{G}$, which is defined in the proof of Theorem 4.2 and the trace function $\rho(c^2-c)$ of the pull back of the Kummer sheaf $\mathcal{L}_\rho$ by the map $c \to c^2-c$. Let $\mathcal{K} = \beta^*\mathcal{L}_\rho$, where the map β is multiplicative translate by $c-1$. We divide the trace function of $\mathcal{G}$ by $\sqrt{p}$. Note that $\mathcal{G}$ is a geometrically irreducible sheaf of rank 2. So the geometrically irreducible, rank 1 sheaf $\mathcal{K}$ is not geometrically isomorphic to the dual of $\mathcal{G}$, which is self dual. Hence form Theorem 1.1 we have

$$\frac{1}{p}\sum_{c=1}^{p-1} \rho(c^2-c)\frac{\phi(a^2c)}{\sqrt{p}} = O\left(\frac{(C(\mathcal{G}))^2(C(\mathcal{K}))^2}{p^{1/2}}\right)$$

which implies

$$\sum_{c=1}^{p-1} \rho(c^2-c)\phi(a^2c) = O(p),$$

as both conductors are of $O(1)$. This completes the proof. ■

4.3 Proof of Theorem 4.5 and Theorem 4.6

In this section we prove our main results Theorem 4.5 and Theorem 4.6. Throughout this section, C stands for the constant given by (4.1). We first recall three lemmas from [40] which will be used to prove our main results.

Lemma 4.9. *[40, Lemma 2] For any odd prime p, we have the asymptotic formula*

$$\sum\nolimits'_{\chi(-1)=1}|L(1,\chi)| = \frac{1}{2}\cdot C\cdot p + O(p^{1/2}\cdot \ln p), \tag{4.6}$$

where C is given by (4.1) and $\sum'_{\chi(-1)=1}$ denotes the summation over all non-principal even characters mod p.

Lemma 4.10. *[40, Lemma 1] For any odd prime p, we have*

$$\sum_{a=1}^{p-1}\left|\sum_{\chi\neq\chi_0}\chi(a)|L(1,\chi)|\right| = O(p\cdot\ln p).$$

Lemma 4.11. *[40, Lemma 4] Let p be an odd prime, χ be any non-principal even character mod p. Then for any integer n with $\gcd(n,p)=1$, we have the identity*

$$|G(n,\chi;p)|^2 = 2p + \left(\frac{n}{p}\right)G(1;p)\sum_{a=1}^{p-1}\chi(a)\left(\frac{a^2-1}{p}\right),$$

where $\left(\frac{\bullet}{p}\right)$ is the Legendre symbol.

The next important result is due to Gauss.

Lemma 4.12. *[1, Theorem 9.16] For any integer $q\geq 1$, we have*

$$G(1;q) = \frac{1}{2}\sqrt{q}(1+i)(1+e^{\frac{-\pi iq}{2}}) = \begin{cases}\sqrt{q}, & if \quad q\equiv 1 \pmod 4;\\ 0, & if \quad q\equiv 2 \pmod 4;\\ i\sqrt{q}, & if \quad q\equiv 3 \pmod 4;\\ (1+i)\sqrt{q}, & if \quad q\equiv 0 \pmod 4.\end{cases}$$

Proof of Theorem 4.5. We first note that if χ is an odd character modulo p, then

$$G(n,\chi;p) = \sum_{a=1}^{p}\chi(a)e\left(\frac{na^2}{p}\right) = 0.$$

Thus, for any n with $\gcd(n,p)=1$ we have

$$\sum_{\chi\neq\chi_0}|G(n,\chi;p)|^6\cdot|L(1,\chi)|=\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}|G(n,\chi;p)|^6\cdot|L(1,\chi)|. \tag{4.7}$$

Using Lemma 4.11 we have

$$\begin{aligned}
&\sum_{\chi\neq\chi_0}|G(n,\chi;p)|^6\cdot|L(1,\chi)|\\
&=\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}|G(n,\chi;p)|^6\cdot|L(1,\chi)|\\
&=\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}\left[2p+G(1;p)\left(\frac{n}{p}\right)\sum_{a=1}^{p-1}\chi(a)\left(\frac{a^2-1}{p}\right)\right]^3\cdot|L(1,\chi)|\\
&=\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}\left[8p^3+12p^2G(1;p)\left(\frac{n}{p}\right)\sum_{a=1}^{p-1}\chi(a)\left(\frac{a^2-1}{p}\right)\right.\\
&\qquad+6pG(1;p)^2\left(\sum_{a=1}^{p-1}\chi(a)\left(\frac{a^2-1}{p}\right)\right)^2\\
&\qquad\left.+G(1;p)^3\left(\frac{n}{p}\right)\left(\sum_{a=1}^{p-1}\chi(a)\left(\frac{a^2-1}{p}\right)\right)^3\right]\cdot|L(1,\chi)|.
\end{aligned}$$

The above sum can be written as

$$\begin{aligned}
&\sum_{\chi\neq\chi_0}|G(n,\chi;p)|^6\cdot|L(1,\chi)|\\
&=8p^3\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}|L(1,\chi)|+12p^2G(1;p)\left(\frac{n}{p}\right)A_1+6pG(1;p)^2A_2+G(1;p)^3\left(\frac{n}{p}\right)A_3,
\end{aligned} \tag{4.8}$$

where

$$A_1 = \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \sum_{a=1}^{p-1} \chi(a) \left(\frac{a^2-1}{p}\right) \cdot |L(1,\chi)|;$$

$$A_2 = \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \left(\sum_{a=1}^{p-1} \chi(a) \left(\frac{a^2-1}{p}\right)\right)^2 \cdot |L(1,\chi)|;$$

$$A_3 = \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \left(\sum_{a=1}^{p-1} \chi(a) \left(\frac{a^2-1}{p}\right)\right)^3 \cdot |L(1,\chi)|.$$

We will now evaluate A_1, A_2 and A_3 one by one. We have the identities

$$\begin{aligned}
&\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi(ab) \left(\frac{a^2-1}{p}\right)\left(\frac{b^2-1}{p}\right) \\
&= \sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi(a) \left(\frac{a^2\bar{b}^2-1}{p}\right)\left(\frac{b^2-1}{p}\right) \\
&= \sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi(a) \left(\frac{a^2-b^2}{p}\right)\left(\frac{b^2-1}{p}\right) \\
&= 2\left(\frac{-1}{p}\right)(p-3) + \sum_{a=2}^{p-2}\sum_{b=1}^{p-1} \chi(a) \left(\frac{a^2-b^2}{p}\right)\left(\frac{b^2-1}{p}\right) \qquad (4.9)
\end{aligned}$$

and

$$\begin{aligned}
&\sum_{a=2}^{p-2} \left(\frac{a^2-b^2}{p}\right) \sum_{\chi(-1)=-1} \chi(a)\,|L(1,\chi)| \\
&\qquad = \sum_{a=1}^{p-1} \left(\frac{a^2-1}{p}\right) \sum_{\chi(-1)=-1} \chi(a)\,|L(1,\chi)| = 0. \qquad (4.10)
\end{aligned}$$

Also, we have the Weil estimate

$$\sum_{b=1}^{p-1} \left(\frac{b^2-a^2}{p}\right)\left(\frac{b^2-1}{p}\right) \leq 3\sqrt{p}, \qquad a^2 \not\equiv 1 \pmod{p}. \qquad (4.11)$$

Applying Lemma 4.10 we directly get

$$A_1 = O(p \cdot \ln p). \tag{4.12}$$

Next using (4.9), we rewrite A_2 as

$$\begin{aligned} A_2 &= \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \left(\sum_{a=1}^{p-1} \chi(a) \left(\frac{a^2-1}{p} \right) \right)^2 \cdot |L(1,\chi)| \\ &= 2 \left(\frac{-1}{p} \right) (p-3) \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} |L(1,\chi)| \\ &\qquad + \sum_{a=2}^{p-2} \sum_{b=1}^{p-1} \left(\frac{a^2-b^2}{p} \right) \left(\frac{b^2-1}{p} \right) \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \chi(a) |L(1,\chi)| \\ &= 2 \left(\frac{-1}{p} \right) (p-3) \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} |L(1,\chi)| \\ &\qquad + O\left(p^{1/2} \sum_{a=2}^{p-2} \left| \sum_{\chi \neq \chi_0} \chi(a) |L(1,\chi)| \right| \right). \end{aligned} \tag{4.13}$$

Hence Lemma 4.9 and Lemma 4.10 yield

$$A_2 = C \cdot \left(\frac{-1}{p} \right) p^2 + O(p^{3/2} \cdot \ln p). \tag{4.14}$$

Next we rewrite A_3 as

$$\begin{aligned} A_3 &= \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \left(\sum_{a=1}^{p-1} \chi(a) \left(\frac{a^2-1}{p} \right) \right)^3 \cdot |L(1,\chi)| \\ &= 2(p-3) \left(\frac{-1}{p} \right) \sum_{c=1}^{p-1} \left(\frac{c^2-1}{p} \right) \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \chi(c) |L(1,\chi)| \end{aligned}$$

$$+\sum_{a=2}^{p-2}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{a^2-b^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{c^2-1}{p}\right)\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}\chi(ac)|L(1,\chi)|$$

$$=\sum_{a=2}^{p-2}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{a^2-b^2c^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{c^2-1}{p}\right)\sum_{\chi\neq\chi_0}\chi(a)|L(1,\chi)|$$

$$+2\left(\frac{-1}{p}\right)\sum_{c=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{c^2-b^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{c^2-1}{p}\right)\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}|L(1,\chi)|.$$

Now using Lemma 4.10 and Theorem 4.4 we obatin

$$\left|\sum_{a=2}^{p-2}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{a^2-b^2c^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{c^2-1}{p}\right)\sum_{\chi\neq\chi_0}\chi(a)|L(1,\chi)|\right|$$

$$\leq\sum_{a=2}^{p-2}\left|\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{a^2-b^2c^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{c^2-1}{p}\right)\right|\left|\sum_{\chi\neq\chi_0}\chi(a)|L(1,\chi)|\right|$$

$$\ll p^2\cdot\ln p.$$

Using Lemma 4.9, Theorem 4.4 and the above estimate we obtain

$$A_3=O(p^2\cdot\ln p). \tag{4.15}$$

Finally, combining (4.8), (4.12), (4.14) and (4.15) for all the prime p satisfying $p\equiv 1 \pmod 4$, and then employing Lemma 4.9 we deduce the required asymptotic formula. ■

Proof of Theorem 4.6. Similarly as (4.7), for any n with $\gcd(n,p)=1$ we have

$$\sum_{\chi\neq\chi_0}|G(n,\chi;p)|^8\cdot|L(1,\chi)|=\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}|G(n,\chi;p)|^8\cdot|L(1,\chi)|.$$

Lemma 4.11 yields

$$\begin{aligned}
&\sum_{\chi\neq\chi_0} |G(n,\chi;p)|^8 \cdot |L(1,\chi)| \\
&\quad = \sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} |G(n,\chi;p)|^8 \cdot |L(1,\chi)| \\
&\quad = \sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \left[2p + G(1;p)\left(\frac{n}{p}\right)\sum_{a=1}^{p-1}\chi(a)\left(\frac{a^2-1}{p}\right)\right]^4 \cdot |L(1,\chi)| \\
&\quad = \sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \Bigg[16p^4 + 32p^3 G(1;p)\left(\frac{n}{p}\right)\sum_{a=1}^{p-1}\chi(a)\left(\frac{a^2-1}{p}\right) \\
&\qquad\qquad +24p^2 G(1;p)^2\left(\sum_{a=1}^{p-1}\chi(a)\left(\frac{a^2-1}{p}\right)\right)^2 \\
&\qquad\qquad +8pG(1;p)^3\left(\frac{n}{p}\right)\left(\sum_{a=1}^{p-1}\chi(a)\left(\frac{a^2-1}{p}\right)\right)^3 \\
&\qquad\qquad +G(1;p)^4\left(\sum_{a=1}^{p-1}\chi(a)\left(\frac{a^2-1}{p}\right)\right)^4\Bigg] \cdot |L(1,\chi)|.
\end{aligned}$$

We write

$$\begin{aligned}
\sum_{\chi\neq\chi_0} |G(n,\chi;p)|^8 \cdot |L(1,\chi)| &= 16p^4 \sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} |L(1,\chi)| + 32p^3 G(1;p)\left(\frac{n}{p}\right) B_1 \\
&\quad +24p^2 G(1;p)^2 B_2 + 8pG(1;p)^3\left(\frac{n}{p}\right) B_3 + G(1;p)^4 B_4, \qquad (4.16)
\end{aligned}$$

where

$$B_1 = \sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \sum_{a=1}^{p-1} \chi(a)\left(\frac{a^2-1}{p}\right) \cdot |L(1,\chi)|;$$

$$B_2 = \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \left(\sum_{a=1}^{p-1} \chi(a) \left(\frac{a^2-1}{p} \right) \right)^2 \cdot |L(1,\chi)|;$$

$$B_3 = \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \left(\sum_{a=1}^{p-1} \chi(a) \left(\frac{a^2-1}{p} \right) \right)^3 \cdot |L(1,\chi)|;$$

$$B_4 = \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \left(\sum_{a=1}^{p-1} \chi(a) \left(\frac{a^2-1}{p} \right) \right)^4 \cdot |L(1,\chi)|.$$

Notice that $A_1 = B_1$. Hence from (4.12) we readily obtain

$$B_1 = O(p \cdot \ln p). \tag{4.17}$$

Similarly, we have $A_2 = B_2$. Hence from (4.14) we find that

$$B_2 = \begin{cases} C \cdot p^2 + O(p^{3/2} \cdot \ln p); & \text{if } p \equiv 1 \pmod 4; \\ -C \cdot p^2 + O(p^{3/2} \cdot \ln p); & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{4.18}$$

Again we have $A_3 = B_3$, thus from (4.15) we readily obtain

$$B_3 = O(p^2 \cdot \ln p). \tag{4.19}$$

Finally, using (4.9) we rewrite B_4 as

$$\begin{aligned} B_4 &= \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \left(\sum_{a=1}^{p-1} \chi(a) \left(\frac{a^2-1}{p} \right) \right)^4 \cdot |L(1,\chi)| \\ &= 4(p-3)^2 \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} |L(1,\chi)| \\ &\quad + 4(p-3) \left(\frac{-1}{p} \right) \sum_{a=2}^{p-2} \sum_{b=1}^{p-1} \left(\frac{a^2-b^2}{p} \right) \left(\frac{b^2-1}{p} \right) \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \chi(a) |L(1,\chi)| \end{aligned}$$

$$+\sum_{a=2}^{p-2}\sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\left(\frac{a^2-b^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{c^2-d^2}{p}\right)\left(\frac{d^2-1}{p}\right)\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}\chi(ac)|L(1,\chi)|$$

$$=(4(p-3)^2+2T)\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}|L(1,\chi)|$$

$$+2(p-3)\left(\frac{-1}{p}\right)\sum_{a=2}^{p-2}\sum_{b=1}^{p-1}\left(\frac{a^2-b^2}{p}\right)\left(\frac{b^2-1}{p}\right)\sum_{\chi\neq\chi_0}\chi(a)|L(1,\chi)|$$

$$+\sum_{a=2}^{p-2}\sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\left(\frac{a^2-b^2c^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{c^2-d^2}{p}\right)\left(\frac{d^2-1}{p}\right)\sum_{\chi\neq\chi_0}\chi(a)|L(1,\chi)|, \tag{4.20}$$

where T is the same as (4.3). From Theorem 4.2 it is easy to see that

$$\sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\left(\frac{a^2-b^2c^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{c^2-d^2}{p}\right)\left(\frac{d^2-1}{p}\right)=O(p^{3/2})$$

for any $a\in\mathbb{F}_p\setminus\{0,\pm1\}$. Using Lemma 4.10 with the above estimate we obtain

$$\left|\sum_{a=2}^{p-2}\sum_{b=1}^{p-1}\sum_{c=2}^{p-2}\sum_{d=1}^{p-1}\left(\frac{a^2-b^2c^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{c^2-d^2}{p}\right)\left(\frac{d^2-1}{p}\right)\sum_{\chi\neq\chi_0}\chi(a)|L(1,\chi)|\right|$$

$$\ll p^{3/2}\sum_{a=2}^{p-2}\left|\sum_{\chi\neq\chi_0}\chi(a)|L(1,\chi)|\right|$$

$$\ll p^{5/2}\cdot\ln p. \tag{4.21}$$

Finally using Lemma 4.9, Lemma 4.10, (4.20) and (4.21) we find that

$$B_4=2\cdot C\cdot p^3+C\cdot T\cdot p+O(p^{5/2}\ln p). \tag{4.22}$$

Combining (4.16), (4.17), (4.18), (4.19) and (4.22), and then employing Lemma 4.9 and the estimate (4.5) we deduce the required asymptotic formula. ■

4.4 Proof of Theorem 4.7 and Theorem 4.8

In this section we prove Theorem 4.7 and Theorem 4.8. The proofs are immediate consequences of Theorem 4.3 and Theorem 4.4.

Proof of Theorem 4.7. Recall from (4.2) that

$$\begin{aligned} N &= \sum_{a=2}^{p-2}\sum_{c=1}^{p-1}\left(\frac{a^2-c^2}{p}\right)\left(\frac{c^2-1}{p}\right)\left(\frac{a^2-1}{p}\right) \\ &= \sum_{a=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{a^2-c^2}{p}\right)\left(\frac{c^2-1}{p}\right)\left(\frac{a^2-1}{p}\right). \end{aligned}$$

We take $a = 1$ in Theorem 4.4 and find that $N = O(p)$. Putting this estimate of N in [18, Theorem 2], we readily obtain the required result. ■

Proof of Theorem 4.8. Recall from (4.3) that

$$T = \sum_{a=2}^{p-2}\sum_{b=1}^{p-1}\sum_{d=1}^{p-1}\left(\frac{a^2-b^2}{p}\right)\left(\frac{b^2-1}{p}\right)\left(\frac{a^2-d^2}{p}\right)\left(\frac{d^2-1}{p}\right).$$

From (4.5) we have

$$T = p^2 + O(p^{3/2}).$$

Putting this estimate of T in [18, Theorem 3], we obtain the required result. ■

4.5 Concluding remarks

We note that the error terms of our theorems are dominated by the error terms of Theorem 4.2, 4.3, 4.4 and Lemma 4.9, 4.10. Hence no further improvements of our results are possible until this part is refined.

We also hope that our new approach can be used to find new higher order

moments of the generalized quadratic Gauss sums, which may be helpful to establish Zhang's conjecture for $m \geq 5$.

5

Bounds on some double exponential sums

5.1 Introduction

In the last chapter we generalize a result of Heath-Brown for double exponential sums. Given sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_p$, we define the following sums

$$S_{a,r,s}(\mathcal{X}, \mathcal{Y}) = \sum_{x \in \mathcal{X}} \left| \sum_{y \in \mathcal{Y}} \mathbf{e}_p \left(a x^r y^s\right) \right|,$$

as defined in (5), for any prime p and integers r and s. Heath-Brown [19] used this sum to give new upper bounds for the first occurance of a positive square free

[1]The contents of this chapter have been accepted for publication in *Journal of Number Theory* (2020).

integer in an arithmetic progression. There is also a large variety of approaches and results about such sums.

For example, in the case of $(r, s) = (-1, -1)$, that is, for incomplete double Kloosterman sums, among other results, Bourgain [6], using methods of additive combinatorics, has given a non-trivial bound of the form $O(XYp^{-\delta})$ provided the length of intervals satisfy $XY \geq p^{1/2+\varepsilon}$ for some fixed $\varepsilon > 0$, where $\delta > 0$ depends only on ε. Here cardinalities of $\mathcal{X}$ and $\mathcal{Y}$ are X and Y respectively.

Below that square-root threshold for the number of terms XY, Bourgain and Garaev [8, Theorem 7], have given a nontrivial estimate of the same form $O(XYp^{-\delta})$ under the conditions

$$X \geq p^{1/18} \qquad \text{and} \qquad Y \geq p^{5/12+\varepsilon}.$$

Note that in [6, 8] the saving δ has never been explicitly evaluated as a function of $\varepsilon > 0$, but there are no principal difficulties to do this.

One can also easily verify that for $s = -2$ and any fixed integer r, using the Hölder inequality, the inequality [19, Equation (21)] and [19, Lemma 1], for an arbitrary set $\mathcal{X} \subseteq \mathbb{F}_p$ of cardinality $\mathcal{X} = X$ and $\mathcal{Y} = \{1, \ldots, Y\}$, with $Y \leq p^{(\ell+1)/2\ell}$ one derives that for any fixed integer $\ell \geq 1$ we have the bound

$$|S_{a,r,-2}(\mathcal{X}, \mathcal{Y})| \leq XY \left(\frac{p}{XY^{2\ell/(\ell+1)}}\right)^{1/2\ell} p^{o(1)}. \tag{5.1}$$

In this chapter we propose a new approach to bounding such sums. The bound we obtain is always weaker than (5.1) however it applies to more general sums, where $\mathcal{Y}$ is not necessary an initial interval but can be in an arbitrary position.

5.2 General notation

For complex weights $\boldsymbol{\alpha} = \{\alpha_s\}_{s\in\mathcal{S}}$, supported on a set $\mathcal{S}$, we define the norms

$$\|\boldsymbol{\alpha}\|_\infty = \max_{s\in\mathcal{S}} |\alpha_s| \qquad \text{and} \qquad \|\boldsymbol{\alpha}\|_\sigma = \left(\sum_{s\in\mathcal{S}} |\alpha_s|^\sigma\right)^{1/\sigma},$$

where $\sigma > 0$.

We use Σ^* to indicate that the poles of rational functions involved are eliminated from the summations domain.

Throughout the chapter, as usual $A \ll B$ is equivalent to the inequality $|A| \leqslant cB$ with some constant $c > 0$, which occasionally, where obvious, may depend on the integer parameters ℓ, r and s. The letter p always denotes a prime number. Finally, to simplify the notation, especially in the exponents, we write $1/ab$ to mean the fraction of the form $1/(ab)$ rather than b/a as the canonical convention requires.

5.3 New bounds of double exponential sums

We consider the following generalisation of the sums $S_{a,r,s}(\mathcal{X}, \mathcal{Y})$. Namely given a sequence of complex weights

$$\boldsymbol{\alpha} = \{\alpha_x\}_{x\in\mathcal{X}},$$

we consider the sums

$$S_{a,r,s}(\boldsymbol{\alpha}; \mathcal{X}, \mathcal{Y}) = \sum_{x\in\mathcal{X}} \alpha_x \sum_{y\in\mathcal{Y}} \mathbf{e}_p\left(ax^r y^s\right).$$

One can certainly write

$$|S_{a,r,s}(\boldsymbol{\alpha}; \mathcal{X}, \mathcal{Y})| \leq \|\boldsymbol{\alpha}\|_\infty S_{a,r,s}(\mathcal{X}, \mathcal{Y}).$$

However we obtain an estimate which is slightly more precise with respect to $\boldsymbol{\alpha}$.

In our argument we consider arbitrary sets $\mathcal{X}$ (and arbitrary intervals $\mathcal{Y}$), hence we can always assume that $r = 1$, and thus it is convenient to define

$$S_{a,s}(\boldsymbol{\alpha}; \mathcal{X}, \mathcal{Y}) = S_{a,1,s}(\boldsymbol{\alpha}; \mathcal{X}, \mathcal{Y}).$$

Theorem 5.1. *Let $\mathcal{X} \subseteq \mathbb{F}_p^*$ be an arbitrary set of cardinality X and let $\mathcal{Y} \subseteq \mathbb{F}_p^*$ be an interval as in (6) of Y consecutive elements. For any fixed nonzero integer s and any complex weights $\boldsymbol{\alpha} = \{\alpha_x\}_{x \in \mathcal{X}}$, for any fixed integer $\ell \geq 1$ if $s < 0$ and for any fixed integer $1 \leq \ell \leq s$ if $s > 0$, we have*

$$|S_{a,s}(\boldsymbol{\alpha}; \mathcal{X}, \mathcal{Y})| \leqslant \|\boldsymbol{\alpha}\|_1^{1-1/\ell} \|\boldsymbol{\alpha}\|_\infty^{1/\ell} X^{1/2\ell} Y \left(Y^{-1/\ell} p^{(\ell+1)/2\ell^2} + 1\right) p^{o(1)}.$$

For the weights with $\|\boldsymbol{\alpha}\|_\infty = p^{o(1)}$ the bound of Theorem 5.1 takes the form

$$|S_{a,s}(\boldsymbol{\alpha}; \mathcal{X}, \mathcal{Y})| \leqslant XY \left(\frac{p^{1+1/\ell}}{XY^2} + \frac{1}{X}\right)^{1/2\ell} p^{o(1)},$$

which is nontrivial when for example, $s < 0$ and for some fixed $\varepsilon > 0$ we have

$$XY^2 \geq p^{1+\varepsilon} \qquad \text{and} \qquad X \geq p^{\varepsilon}.$$

For $Y \leq p^{(\ell+1)/2\ell}$ this bound becomes

$$|S_{a,s}(\boldsymbol{\alpha}; \mathcal{X}, \mathcal{Y})| \leqslant XY \left(\frac{p^{1+1/\ell}}{XY^2}\right)^{1/2\ell} p^{o(1)},$$

which is always weaker than (5.1) if $s = -2$, however it applies in a wider range and of course to more general sums.

5.4 Multiplicative congruences with intervals

We need the following simple statement given in [9, Theorem 4.1.], which is based on a result of Ayyad, Cochrane and Zheng [2, Theorem 1], see also [25] for a slightly more general statement.

Lemma 5.2. *Let $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p^*$ be two intervals as in (6) containing U, V consecutive residues modulo p, respectively. Then for any fixed nonzero integers r and s we have*

$$\#\{(u_1, u_2, v_1, v_2) \in \mathcal{U}^2 \times \mathcal{V}^2 : u_1^r v_1^s \equiv u_2^r v_2^s \pmod p\} \ll \frac{U^2V^2}{p} + UVp^{o(1)}.$$

We now derive a version of an estimate, which was obtained and used in [28, Section 4.2] and [29, Section 2.2] for initial intervals.

Lemma 5.3. *Let $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p^*$ be two intervals as in (6) containing U, V consecutive residues modulo p, respectively, and let $\mathcal{W} \subseteq \mathbb{F}_p$ be an arbitrary set of cardinality W. Then for any fixed non-zero integers r, s and t we have*

$$\begin{aligned}\#\{(u_1, u_2, v_1, v_2, w_1, w_2) \in \mathcal{U}^2 \times \mathcal{V}^2 \times \mathcal{W}^2 :& \\ u_1^r v_1^s \equiv u_2^r v_2^s \pmod p \ \&\ u_1^t w_1 \equiv u_2^t w_2 \pmod p\}& \\ \le UVW\left(\frac{UV}{p} + 1\right)p^{o(1)}.&\end{aligned}$$

Proof. When a solution to the congruence $u_1^r v_1^s \equiv u_2^r v_2^s \pmod p$ is fixed, for each w_1 there are at most one possible value for w_2, which satisfies $u_1^t w_1 \equiv u_2^t w_2 \pmod p$. The result now follows from the bound of Lemma 5.2. ∎

5.5 Proof of the main result

We fix two positive parameters U and V with

$$UV \leqslant Y. \tag{5.2}$$

Let $\mathcal{U}$ and $\mathcal{V}$ be the sets of integers in the intervals $[U/2, U]$ and $[V/2, V]$, respectively.

We write

$$S_{a,s}(\boldsymbol{\alpha}; \mathcal{X}, \mathcal{Y}) = \frac{1}{\#\mathcal{U}\#\mathcal{V}} \sum_{x \in \mathcal{X}} \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \sideset{}{^*}\sum_{\substack{y=A-Y \\ y-uv \in \mathcal{Y}}}^{A+2Y} \alpha_x \, \mathbf{e}_p(x(y-uv)^s),$$

where we recall that Σ^* always indicates that the poles of the rational function in the exponent are eliminated from the summations (in this particular case the values of y with $\gcd(y-uv, p) > 1$).

Applying the same transformation as in the work of Fouvry and Michel [16, Equations (4.3) and (4.4)] and see that for some real ξ we have

$$S_{a,s}(\boldsymbol{\alpha}; \mathcal{X}, \mathcal{Y}) \ll \frac{\log p}{UV} \sum_{x \in \mathcal{X}} \sum_{u \in \mathcal{U}} \sideset{}{^*}\sum_{y=A-Y}^{A+2Y} |\alpha_x| \left| \sum_{v \in \mathcal{V}} \mathbf{e}_p(x(y-uv)^s) \, \mathbf{e}(\xi v) \right|.$$

Using our choice $u \in \mathbb{F}_p^*$, we now further write it as

$$S_{a,s}(\boldsymbol{\alpha}; \mathcal{X}, \mathcal{Y}) \ll \frac{\log p}{UV} \mathfrak{S}, \tag{5.3}$$

where

$$\mathfrak{S} = \sum_{x \in \mathcal{X}} \sum_{u \in \mathcal{U}} \sum_{y=A-Y}^{A+2Y} |\alpha_x| \left| \sideset{}{^*}\sum_{v \in \mathcal{V}} \mathbf{e}_p\left(u^s x \left(yu^{-1} - v\right)^s\right) \mathbf{e}(\xi v) \right|.$$

Now, similarly to [28], we collect together the triples (u, x, y) with set same values $\lambda \equiv u^s x \pmod p$ and $\mu \equiv yu^{-1} \pmod p$. More precisely for $(\lambda, \mu) \in \mathbb{F}_p^2$ we

define

$$\nu(\lambda,\mu)=\sum_{\substack{x\in\mathcal{X},\ u\in\mathcal{U},\ y\in[A-Y,A+2Y]\\ (u^s x,yu^{-1})\equiv(\lambda,\mu)\pmod p}}\ldots\sum|\alpha_x|.$$

Hence we have

$$\mathfrak{S}\leqslant\sum_{(\lambda,\mu)\in\mathbb{F}_p^2}\nu(\lambda,\mu)\left|\sum_{v\in\mathcal{V}}^{*}\mathbf{e}_p\left(\lambda\left(\mu-v\right)^s\right)\mathbf{e}(\xi v)\right|. \tag{5.4}$$

We trivially have

$$\sum_{(\lambda,\mu)\in\mathbb{F}_p^2}\nu(\lambda,\mu)\ll\|\boldsymbol{\alpha}\|_1 UY. \tag{5.5}$$

Furthermore, by Lemma 5.3 we have

$$\sum_{(\lambda,\mu)\in\mathbb{F}_p^2}\nu(\lambda,\mu)^2\ll\|\boldsymbol{\alpha}\|_\infty^2 UXY\left(\frac{UY}{p}+1\right)p^{o(1)} \tag{5.6}$$

for any set $\mathcal{X}$.

Let us fix some integer $\ell\geqslant 1$. Writing (5.4) as,

$$\mathfrak{S}\leqslant\sum_{(\lambda,\mu)\in\mathbb{F}_p^2}\nu(\lambda,\mu)^{(\ell-1)/\ell}\nu(\lambda,\mu)^{1/\ell}\left|\sum_{v\in\mathcal{V}}^{*}\mathbf{e}_p\left(\lambda\left(\mu-v\right)^s\right)\mathbf{e}(\xi v)\right|,$$

by the Hölder inequality, and also using (5.5) and (5.6), we obtain

$$\begin{aligned}\mathfrak{S} &\le \left(\sum_{(\lambda,\mu)\in\mathbb{F}_p^2}\nu(\lambda,\mu)\right)^{1-1/\ell}\left(\sum_{(\lambda,\mu)\in\mathbb{F}_p^2}\nu(\lambda,\mu)^2\right)^{1/2\ell}\\ &\qquad\left(\sum_{(\lambda,\mu)\in\mathbb{F}_p^2}\left|\sum_{v\in\mathcal{V}}^{*}\mathbf{e}_p\left(\lambda\left(\mu-v\right)^s\right)\mathbf{e}(\xi v)\right|^{2\ell}\right)^{1/2\ell}\\ &\le \|\boldsymbol{\alpha}\|_1^{1-1/\ell}\|\boldsymbol{\alpha}\|_\infty^{1/\ell}(UY)^{1-1/\ell}(UXY)^{1/2\ell}\\ &\qquad\left(U^{1/2\ell}Y^{1/2\ell}p^{-1/2\ell}+1\right)W^{1/2\ell}p^{o(1)},\\ &= \|\boldsymbol{\alpha}\|_1^{1-1/\ell}\|\boldsymbol{\alpha}\|_\infty^{1/\ell}U^{1-1/2\ell}Y^{1/2\ell}Y^{1-1/2\ell}\\ &\qquad\left(U^{1/2\ell}Y^{1/2\ell}p^{-1/2\ell}+1\right)W^{1/2\ell}p^{o(1)},\end{aligned} \tag{5.7}$$

where

$$W=\sum_{(\lambda,\mu)\in\mathbb{F}_p^2}\left|\sum_{v\in\mathcal{V}}^{*}\mathbf{e}_p\left(\lambda\left(\mu-v\right)^s\right)\mathbf{e}(\xi v)\right|^{2\ell}.$$

Opening up the inner sum, changing the order of summation and using the orthogonality of exponential functions, we obtain

$$W=\sum_{v_1,\dots,v_{2\ell}\in\mathcal{V}}\dots\sum\mathbf{e}\left(\xi\sum_{j=1}^{2\ell}(-1)^j v_j\right)\sum_{\mu\in\mathbb{F}_p}\sum_{\lambda\in\mathbb{F}_p}\mathbf{e}_p\left(\lambda\sum_{j=1}^{2\ell}(-1)^j\left(\mu-v_j\right)^s\right).$$

Since the inner sum over $\lambda\in\mathbb{F}_p$ vanishes unless

$$\sum_{j=1}^{2\ell}(-1)^j\left(\mu-v_j\right)^s\equiv 0 \pmod p \tag{5.8}$$

(in which case it is equal to p), we obtain

$$W\leqslant pT, \tag{5.9}$$

where T is the number of solutions to (5.8) in variables $\mu\in\mathbb{F}_p$ and $v_1,\dots,v_{2\ell}\in\mathcal{V}$.

Consider the rational function

$$F(Z) = \sum_{j=1}^{2\ell} (-1)^j \, (Z - v_j)^s \in \mathbb{F}_p[Z].$$

We now notice that if $s < 0$ or $s > 0$ and $\ell \leq s$, then $F(Z)$ vanishes identically only if the vectors

$$(v_1, v_3, \ldots, v_{2\ell-1}) \qquad \text{and} \qquad (v_2, v_4, \ldots, v_{2\ell})$$

are permutations of each other. Indeed, if $s < 0$, then we can see this from examining the poles of $F(Z)$. If $s > 0$ and $\ell \leq s$, then $F(Z)$ vanishes if and only if

$$\sum_{j=1}^{2\ell} (-1)^j v_j^i = 0, \qquad i = 1, \ldots, s,$$

and using the Newton formulas relating power sums to elementary symmetric functions we see that $v_1, v_3, \ldots, v_{2\ell-1}$ and $v_2, v_4, \ldots, v_{2\ell}$ are roots of the same polynomial of degree ℓ and thus are permutations of each other.

If $F(Z)$ vanishes, then there are p admissible values for μ to satisfy (5.8). Otherwise there are $O(1)$ choices for μ. Hence

$$T \ll pV^{\ell} + V^{2\ell}. \tag{5.10}$$

We now choose

$$V = p^{1/\ell} \qquad \text{and} \qquad U = Yp^{-1/\ell}, \tag{5.11}$$

thus the condition (5.2) is satisfied. Now, with the choice (5.11) the bound (5.10) becomes $T \ll V^{2\ell}$. Therefore, from (5.9) we obtain

$$W \leqslant pV^{2\ell}.$$

Substituting this bound in (5.7), we derive

$$\mathfrak{S} \leqslant \|\boldsymbol{\alpha}\|_1^{1-1/\ell}\|\boldsymbol{\alpha}\|_\infty^{1/\ell}U^{1-1/2\ell}VX^{1/2\ell}Y^{1-1/2\ell}p^{1/2\ell+o(1)}\left(U^{1/2\ell}Y^{1/2\ell}p^{-1/2\ell}+1\right).$$

Recalling (5.3), we derive

$$|S_{a,s}(\boldsymbol{\alpha};\mathcal{X},\mathcal{Y})| \leqslant \|\boldsymbol{\alpha}\|_1^{1-1/\ell}\|\boldsymbol{\alpha}\|_\infty^{1/\ell}U^{-1/2\ell}X^{1/2\ell}Y^{1-1/2\ell}p^{1/2\ell+o(1)}\left(U^{1/2\ell}Y^{1/2\ell}p^{-1/2\ell}+1\right),$$

and with the choice (5.11), we conclude the proof.

Bibliography

[1] T. M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York-Heidelberg, 1976. Undergraduate Texts in Mathematics.

[2] 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(2):398–413, 1996.

[3] V. Blomer, É. Fouvry, E. Kowalski, P. Michel, and D. Milićević. On moments of twisted L-functions. *Amer. J. Math.*, 139(3):707–768, 2017.

[4] V. Blomer, É. Fouvry, E. Kowalski, P. Michel, D. Milićević, and W. Sawin. The second moment theory of families of L-functions. *Memoirs Amer. Math. Soc. (to appear)*.

[5] V. Blomer and D. Milićević. The second moment of twisted modular L-functions. *Geom. Funct. Anal.*, 25(2):453–516, 2015.

[6] J. Bourgain. More on the sum-product phenomenon in prime fields and its applications. *Int. J. Number Theory*, 1(1):1–32, 2005.

[7] J. Bourgain and M. Z. Garaev. Kloosterman sums in residue rings. *Acta Arith.*, 164(1):43–64, 2014.

[8] Zh. Burgeĭn and M. Z. Garaev. Sumsets of reciprocals in prime fields and multilinear Kloosterman sums. *Izv. Ross. Akad. Nauk Ser. Mat.*, 78(4):19–72, 2014.

[9] J. Cilleruelo, I. E. Shparlinski, and A. Zumalacárregui. Isomorphism classes of elliptic curves over a finite field in some thin families. *Math. Res. Lett.*, 19(2):335–343, 2012.

[10] T. Cochrane. Exponential sums and the distribution of solutions of congruences. *Lecture notes delivered at the Institute of Mathematics, Academia Sinica, Taipei, Taiwan*, pages 1–84, 1994.

[11] T. Cochrane and Z. Zheng. Pure and mixed exponential sums. *Acta Arith.*, 91(3):249–278, 1999.

[12] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[13] P. Deligne. Applications de la formule des traces aux sommes trigonométriques. In *Cohomologie étale*, volume 569 of *Lecture Notes in Math.*, pages 168–232. Springer, Berlin, 1977.

[14] P. Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52):137–252, 1980.

[15] É. Fouvry, E. Kowalski, P. Michel, and W. Sawin. Lectures on applied ℓ-adic cohomology. In *Analytic methods in arithmetic geometry*, volume 740 of *Contemp. Math.*, pages 113–195. Amer. Math. Soc., Providence, RI, 2019.

[16] É. Fouvry and P. Michel. Sur certaines sommes d'exponentielles sur les nombres premiers. *Ann. Sci. École Norm. Sup. (4)*, 31(1):93–130, 1998.

[17] J. B. Friedlander and H. Iwaniec. Incomplete Kloosterman sums and a divisor problem. *Ann. of Math. (2)*, 121(2):319–350, 1985. With an appendix by Bryan J. Birch and Enrico Bombieri.

[18] Y. He and Q. Liao. On an identity associated with Weil's estimate and its applications. *J. Number Theory*, 129(5):1075–1089, 2009.

[19] D. R. Heath-Brown. The least square-free number in an arithmetic progression. *J. Reine Angew. Math.*, 332:204–220, 1982.

[20] H. Iwaniec. *Topics in classical automorphic forms*, volume 17 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1997.

[21] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[22] N. M. Katz. *Sommes exponentielles*, volume 79 of *Astérisque*. Société Mathématique de France, Paris, 1980. Course taught at the University of Paris, Orsay, Fall 1979, With a preface by Luc Illusie, Notes written by Gérard Laumon, With an English summary.

[23] N. M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.

[24] N. M. Katz. *Convolution and equidistribution*, volume 180 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2012. Sato-Tate theorems for finite-field Mellin transforms.

[25] B. Kerr. On the congruence $x_1x_2 \equiv x_3x_4 \mod q$. *J. Number Theory*, 180:154–168, 2017.

[26] H. D. Kloosterman. Asymptotische Formeln für die Fourierkoeffizienten ganzer Modulformen. *Abh. Math. Sem. Univ. Hamburg*, 5(1):337–352, 1927.

[27] H. D. Kloosterman. On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. *Acta Math.*, 49(3-4):407–464, 1927.

[28] E. Kowalski, P. Michel, and W. Sawin. Bilinear forms with generalized Kloosterman sums. *Ann. Scoula Normale Pisa (to appear)*.

[29] E. Kowalski, P. Michel, and W. Sawin. Bilinear forms with Kloosterman sums and applications. *Ann. of Math. (2)*, 186(2):413–500, 2017.

[30] S. Lang and A. Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954.

[31] W. Luo. Bounds for incomplete hyper-Kloosterman sums. *J. Number Theory*, 75(1):41–46, 1999.

[32] W. Luo, Z. Rudnick, and P. Sarnak. On Selberg's eigenvalue conjecture. *Geom. Funct. Anal.*, 5(2):387–401, 1995.

[33] L. J. Mordell. On a special polynomial congruence and exponential sum. In *Calcutta Math. Soc. Golden Jubilee Commemoration Vol*, pages 29–32. Calcutta Math. Soc., Calcutta, 1963.

[34] H. Poincaré. Fonctions modulaires et fonctions fuchsiennes. *Ann. Fac. Sci. Toulouse Sci. Math. Sci. Phys. (3)*, 3:125–149, 1911.

[35] I. E. Shparlinski. Bounds of incomplete multiple Kloosterman sums. *J. Number Theory*, 126(1):68–73, 2007.

[36] R. A. Smith. On n-dimensional Kloosterman sums. *J. Number Theory*, 11(3, S. Chowla Anniversary Issue):324–343, 1979.

[37] A. Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U.S.A.*, 34:204–207, 1948.

[38] Y. Ye. Identities of incomplete Kloosterman sums. *Proc. Amer. Math. Soc.*, 127(9):2591–2600, 1999.

[39] M. P. Young. The fourth moment of Dirichlet L-functions. *Ann. of Math. (2)*, 173(1):1–50, 2011.

[40] W. P. Zhang. Moments of generalized quadratic Gauss sums weighted by L-functions. *J. Number Theory*, 92(2):304–314, 2002.

[41] W. P. Zhang and X. X. Li. The fourth power mean of the general 2-dimensional Kloostermann sums mod p. *Acta Math. Sin. (Engl. Ser.)*, 33(6):861–867, 2017.

[42] W. P. Zhang and X. X. Lv. The fourth power mean of the general 3-dimensional Kloostermann sums mod p. *Acta Math. Sin. (Engl. Ser.)*, 35(3):369–377, 2019.

Publications

Publications from Thesis work

1. N. Bag and R. Barman, An improved estimate of fourth power mean of the general 3-dimensional Kloosterman sum mod p, *Funct. Approx. Comment. Math.*, accepted for publication, doi:10.7169/facm/1872.

2. N. Bag and R. Barman, Fourth power mean of the general 4-dimensional Kloosterman sum mod p, *Research in Number Theory,* 6 (2020), Article no. 31, 16 pages.

3. N. Bag and R. Barman, Higher order moments of generalized quadratic Gauss sums weighted by L-functions, *Asian Journal of Mathematics*, accepted for publication.

4. N. Bag and I. E. Shparlinski, Bounds of some double exponential sums, *Journal of Number Theory,* 219 (2021), 228-236.

List of symbols

$\mathbb{A}^1_{\mathbb{F}_p}$	Affine line over $\mathbb{F}_p$
$\mathbb{C}$	Set of complex numbers
$\mathbb{F}_q$	Finite field of q elements
$\mathbb{N}$	Set of natural numbers
$\mathbb{P}^1_{\mathbb{F}_p}$	Projective line over $\mathbb{F}_p$
$\mathbb{Q}$	Set of rational numbers
$\mathbb{Q}_\ell$	ℓ-adic numbers
$\mathbb{R}$	Set of real numbers
$\mathbb{Z}$	Set of integers
$\mathrm{Frob}_{k_x}^{arith}$	Arithmetic Frobenius
$\mathrm{Frob}_{k_x}^{geom}$	Geometric Frobenius
Frob_x	Frobenius class at $\{x\}$
$\mathrm{Swan}_x(\mathcal{F})$	Swan conductor of $\mathcal{F}$ at x
$C(\mathcal{F})$	Conductor of $\mathcal{F}$

$C(\mathcal{F}, \mathcal{G})$	Correlation sum between traces of $\mathcal{F}$ and $\mathcal{G}$
$D_{\mathcal{F}}^{ram}$	Set of geometric points where $\varrho_{\mathcal{F}}$ is ramified
$D_{\{x\}}$	Decomposition group
$G(n, \chi; q)$	Generalized quadratic Gauss sum
$G(n; q)$	Classical quadratic Gauss sum
G^{arith}	Arithmetic Galois group
G^{geom}	Geometric Galois group
$I_{\{x\}}$	Inertia group
$K(m, s, \chi; q)$	General s-dimensional Kloosterman sum
$K(m, s; q)$	Hyper-Kloosterman sum
k_x	Residue field
$K_{\mathcal{F}}$	Trace function associated to $\mathcal{F}$
$L(s, \chi)$	Dirichlet L-function
$R[X]$	Polynomial ring over a ring R
$S(a, b; q)$	Classical Kloosterman sum
$S_{a,r,s}(\mathcal{X}, \mathcal{Y})$	Double exponential sum
v_x	Discrete valuation
Z_Q	Closed set, set of zeroes of some polynomial Q

Index

Appendix: Deligne's Proof of Lemma 3.4

I played with your surface (with $u \neq 0$)

$$(x-1)(y-1)(z-1)(1-xyz) - u\,xyz = 0 \qquad (1)$$

It is a beautiful surface, but its analysis tells that its number of points should not be $p^2 + O(p^{1/2})$, but rather $p^2 + O(p)$. Here is the story.

On this surface, we have the 6 lines where one coordinate is 0 — equivalently, one coordinate is 1. They meet in the six points S_3-conjugate of $(0,0,1)$ or $(1,1,0)$, where two lines meet. The union of the 6 lines has hence $6p - 6$ points (over $\mathbb{F}_q$: $6q - 6$). If we remove them, and put $t = 1/xyz$, we have the more symetric form :

$$\text{In } \mathbb{G}_m^4, \quad \begin{cases} xyzt = 1 \\ (x-1)(y-1)(z-1)(t-1) = u \end{cases} \qquad (2)$$

where the 4 coordinates play symmetric roles : S_4-symmetry. We have the additional symmetry

$$z = (x, y, z, t) \longrightarrow (1/x, 1/y, 1/z, 1/t).$$

To compactify, preserving the symmetry, one should embed $\mathbb{G}_m^4$ into $(\mathbb{P}^1)^4$. If on the i^{th} $\mathbb{P}^1$ we use projective coordinates (x_i, x_i'), (2) is the trace on $\mathbb{G}_m^4 \subset (\mathbb{P}^1)^4$ of the intersection of the hypersurfaces with equations (multihomogeneous of degrés $(1,1,1,1)$

$$\begin{cases} \prod x_i = \prod x_i' \\ \prod (x_i - x_i') = u \prod x_i' \end{cases} \qquad (3)$$

In those coordinates, z is $x_i \leftrightarrow x_i'$.

On $\mathbb{P}^1$, with homogeneous coordinates x, x', $x = 0$ defines the point 0, $x' = 0$ the point ∞ and $x - x' = 0$ the point 1. If $(P_1, P_2, P_3, P_4) \in (\mathbb{P}^1)^4$ is on the surface (3), one P_i is 0 if and only if one other is 1 if and only if a third is ∞ : one obtains the surface (2) from the surface (3) by removing the $\mathbb{P}^1$ in the S_4 - orbit of $\{0\} \times \{1\} \times \{\infty\} \times \mathbb{P}^1 \subset (\mathbb{P}^1)^4$. This set of $\overset{(24}{\vee}\mathbb{P}^1$ is an homogeneous space under the symmetry group $S_4 \times \{1, 2\}$. The stabilizer of the line written above is ~~[illegible]~~ the subgroup

$$\{e, ((1,3), 2)\} .$$

To obtain your surface (1), one removes only ~~[illegible]~~ 18 of the 24 lines : one takes the intersection with

$$(\mathbb{P}^1 - \{\infty\}) \times (\mathbb{P}^1 - \{\infty\}) \times (\mathbb{P}^1 - \{\infty\}) \times (\mathbb{P}^1 - \{0\}) :$$

This means putting $x_1' = x_2' = x_3' = x_4 = 1$ and one takes as coordinates x_1, x_2, x_3, x_4'. The equations become

$$x_1 x_2 x_3 = x_4'$$

$$(x_1 - 1)(x_2 - 1)(x_3 - 1)(1 - x_4') = u\, x_4'$$

which, eliminating x_4', gives (1). The lines among the 24 $\mathbb{P}^1$ which persist in (1) are those mapping to ∞ in the 4^{th} $\mathbb{P}^1$, each meets one point.

The surface (3) is non singular, except for $u = 16$ or $u = -4$, where the following points, contained in G_m^4, are singular :

$$(4)\quad \begin{cases} u = 16 & \text{point } (-1,-1,-1,-1) \\ u = -4 & \text{points } \pm(i,i,i,i) \qquad (\text{where } i = \sqrt{-1}) \end{cases}$$

This is checked using the Jacobian criterion. Inside G_m^4, we have the two equations (2), and we need to check the non vanishing of a 2×2 minor of

$$\begin{matrix} yzt & xzt & xyt & xyz \\ (y-1)(z-1)(t-1) & (x-1)(z-1)(t-1) & (x-1)(y-1)(t-1) & (x-1)(y-1)(z-1) \end{matrix}$$

Dividing the 1st line by $xyzt$, the second by $(x-1)(y-1)(z-1)(t-1)$, we get

$$\begin{matrix} 1/x & 1/y & 1/z & 1/t \\ 1/x-1 & 1/y-1 & 1/z-1 & 1/t-1 \end{matrix}$$

one has

$$\det\begin{pmatrix} 1/x & 1/y \\ 1/x-1 & 1/y-1 \end{pmatrix} = \frac{1}{xy(x-1)(y-1)}(x-y) \neq 0$$

one gets a singularity only for $x = y = z = t$, leading to (4).

Outside of G_m^4, we have the 24 projective lines $(P_1, P_2, P_3, P_4) \in (\mathbb{P}^1)^4$ where some three of the P_j are $0, 1, \infty$. They are simply transitively permuted by S_4. We also have the symmetry : $x \to x^{-1}$ on all $\mathbb{P}^1$. To check non singularity outside of G_m^4, it hence suffices to do it on the affine line of the $(0, 1, \infty, t)$, $t \neq \infty$.

One can compute in the chart $(\mathbb{A}^1)^4$ with

$x_1' = x_2' = x_3 = x_4' = 1$: coordinates x_1, x_2, x_3', x_4,

rewritten x, y, z', t, equations

$$x\,y\,t - z' = 0$$

$$(x-1)(y-1)(1-z')(t-1) + u\,z' = 0,$$

non singularity to be checked on $x=0, y=1, z'=0$. There, the derivatives in x, y, z' are

$$\begin{matrix} t & 0 & -1 \\ 0 & t-1 & -u \end{matrix}$$

and we always have a non zero 2×2 minor.

If in $(\mathbb{P}^1)^4$ we take the intersection of two hypersurface of degree $(1,1,1,1)$, we get a $K3$ surface (when non singular) : Betti numbers $(1, 0, 22, 0, 1)$. Our surface (3) is hence a $K3$, except that for $u = 16$ (resp -4) it degenerates by acquiring one (resp two) singular points. Special cases : in char. 2 (resp 5), non singularity (always for $u \neq 0$), (resp 3 singular points for $u = 16 = -4 = 1$). Note that outside of G_m^4 we have always the same lines :

ordinary quadratic singularities

24 lines, some three of the coordinates $0, 1, \infty \in \mathbb{P}^1$

intersections : 36 points, the coordinate among $0, 1, \infty$, all three occurring, one of them twice. Over $\mathbb{F}_q$, we hence have for the number of points

$$|(1)| = |(2)| + 6q - 6$$

$$|(3)| = |(2)| + 24(q+1) - 36$$

$$= |(2)| + 24q - 12$$

For me, understanding number of points means understanding cohomology. The action of the symmetry group $S_4 \times \{1,2\}$ breaks ~~adelt~~ $H^2(\text{(3)})$ into pieces, indexed by the irreducible representations of the symmetry group. As for some subgroups H of the symmetry group, surface(3)/H is easy to understand, and that

$$H^*(\text{surface}/H) = H^*(\text{surface})^H,$$

we get a lot of information.

(a) $H = S_4$: Here, $(\mathbb{P}^1)^4/H = \mathbb{P}^4$, and to get $(\text{(3)}/H)$, we have to take the intersection of two hyperplanes : we get a $\mathbb{P}^2$

(b) $H = S_3$ permuting 1,2,3 Here $\mathbb{P}^{1\,4}/H = \mathbb{P}^3 \times \mathbb{P}^1$, and we have to take the intersection of two hypersurfaces of bidegree (1,1) : we get a fiber space over $\mathbb{P}^1$ with fiber $\mathbb{P}^1$

On $(\mathbb{P}^1)^4$, we have the four line bundles inverse image of $\mathcal{O}(1)$ on $\mathbb{P}^1$, with Chern class $c_1(p_i^*\mathcal{O}(1))$ noted η_i. The S_4 - invariant class in $H^2(\text{surface (3)})$ is $\eta_1 + \eta_2 + \eta_3 + \eta_4$, and for the S_3 - invariant class, S_3 permuting $\{1,2,3,4\} - \{i\}$, we get in addition η_i

Note that ~~fo~~ all the η_i are fixed by τ

The only irreducible representations of S_4 with a vector fixed by S_3 are $\square\square\square\square$ and $\begin{array}{|c|}\hline\square\\\hline\square\\\hline\end{array}$, whose sum is the permutation representation.

We conclude that in $H^2(\text{surface }(3))$ decomposed into irreducible representation of $S_4 \times \{1, z\}$, we have one summand $\square\square\square\square$, $z=1$ and one $\begin{array}{|c|}\hline\square\\\hline\square\\\hline\end{array}$, $z=1$, sum corresponding to the permutation representation on the η_c.

The rest (=orthogonale) has no representation $\square\square\square\square$ or $\begin{array}{|c|}\hline\square\\\hline\square\\\hline\end{array}$ of S_4.

ⓒ $H = S_2$, permuting 1, 2. Here, $(\mathbb{P}^1)^4/H = \mathbb{P}^2 \times \mathbb{P}^1 \times \mathbb{P}^1$

What happens on the $(\mathbb{G}_m^4$ - part of $(3))/H$ is easy: it maps isomorphically to $(\mathbb{P}^1 - \{0, 1, \infty\})^2$: in the coordinates on $(\mathbb{G}_m^4)/H$ $\sigma_1 = x+y$, $\sigma_2 = xy$, z, t the equations are $\sigma_2 z t = 1$, $(\sigma_2 - \sigma_1 + 1)(z-1)(t-1) = u$, with σ_1, σ_2 determined by z, t. However, for

$$(\text{surface }(3))/H \longrightarrow \mathbb{P}^1 \times \mathbb{P}^1,$$

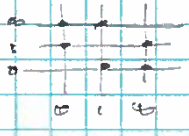
we have some blowing up: above (P_1, P_2) in $\mathbb{P}^1 \times \mathbb{P}^1$ with P_1, P_2 distinct and among $0, 1, \infty$, (3) consists of 2 projective lines meeting in one point, for instance

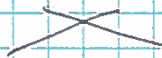
$$(0, 1, \infty, *) \cup (0, 1, *, \infty) \longrightarrow (0, 1).$$

The two lines are permuted by H, so that above each of the 6 points (P_1, P_2) we have a projective line.

We get:

$$(\text{surface }(3)/H) \xrightarrow{\sim} \mathbb{P}^1 \times \mathbb{P}^1 \text{ blown up at the 6 points:}$$



This can be used to give a picture of the surface (3) : it is a double covering of $\mathbb{P}^1 \times \mathbb{P}^1$, ramified along a curve of bidegree (4,4) with a ~~node~~ cusp at each of the 6 points in question. Taking the finite double covering with this ramification, we get a A_2 singularity ~~at ∞~~ above each of the 6 points, which resolves with exceptional divisor  .

One also see that by projecting further to one of the $\mathbb{P}^1$, (3) is an elliptic fibration, ~~with the points~~ with above $0, 1, \infty$ on preimage of $\mathbb{P}^1$ 

[for instance, for (3) $\to$ 1st $\mathbb{P}^1$, above 0, we have  above $(0,1)$, above $(0,\infty)$ and the disjoint lines  $(0,*,1,\infty)$ $(0,*,\infty,1)$ above $(0,*)$. Above $\mathbb{P}^1 = (a,*)$, the elliptic fiber at a is a double covering ramified at the 4 points (sometime colleding) intersection of $(a,*)$ with the ramification curve of degree (4,4).

More important for me, we get a description of the invariants of S_2 (permuting 1,2) on H^2(surface (3)), giving how

$$S_2 \text{ (permuting 3,4)} \times \{1, z\}$$

acts on $H^2((3))^H$. Indeed, S_2 (permuting 3,4) acts by permuting the two factors $\mathbb{P}^1$, while z acts by $x \mapsto x^{-1}$ on each

One obtains that as a representation of

$$S_2 \ (3 \leftrightarrow 4) \times \{1,2\}, \qquad H^2(\text{surface}(3))^H$$

is as follows:

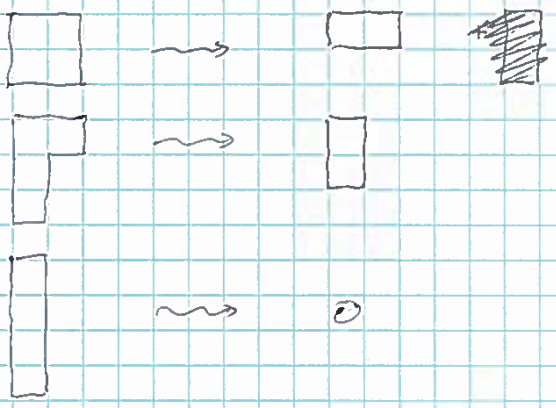
from $c_1(pr_3^* \mathcal{O}(1))$, $c_2(pr_4^* \mathcal{O}(1))$:

$2 \times$ trivial ($\square\square$), $z=1$

From the 6 blown up points :

$2 \times \square$, $z=1$ $\quad 2 \times \square$, $z=-1$ $\quad 1 \times \square$ $z=-1$ $\quad 1 \times \square$ $z=1$

The permutation representation $\square\square + \square\!\square$ on the η_i contributes the 1st line + $\square$, $z=1$ once part. ~~As by restriction from S_4 to S_2~~ ~~we~~ As when we take the invariants by S_2 $\{1 \leftrightarrow 2\}$ of a representation of S_4, the representation of S_2 $\{3 \leftrightarrow 4\}$ we get is



We find that the representation of S_4 on H^2 is

$\square\square$ $z=1$ $+$ $\square\!\square$ $z=1$: permutation of the η_i

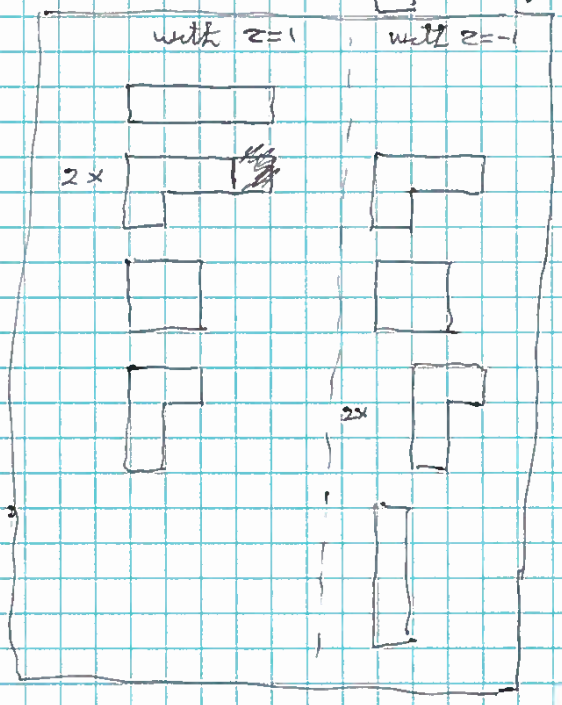
$+$ $\square$ $z=1$ $+$ $\square$ $z=-1$

$+$ $\square\!\square$ $z=-1$ $+ 2$ $\square\!\square$ $z=-1$

plus a number of sign representations of S_4 :

All the representations of S_4 in H^2 considered so far (those with a fixed vector by S_2) are contained in the span of the class of the 24 lines outside G_m^4. This span is the image of a regular representation of S_4. In this image, the sign representation occurs (once) : the alternating sum of the 24 lines has a non zero square [= -120]

The representation of $S_4 \times \{1,2\}$ on the set of the 24 lines $\mathbb{Z}^{(\text{set of lines})}$ admits as one stabiliser the diagonal subgroup in $S_2 \times \{1,2\}$; ~~it is~~ the corresponding permutation representation is induced from $\left(\square, z=1 \oplus \square, z=-1\right)$ of $S_2 \times \{1,2\}$. It is



Comparing with H^2, we see that they are relations among the classes of the lines ; As representation of the symmetry group, the span of the lines is the quotient of $\mathbb{Z}^{\{\text{lines}\}}$ by one $\square$ ($z=1$) and one $\begin{smallmatrix}\square\\\square\end{smallmatrix}$ ($z=-1$).

The span of the 24 lines in H^2 is hence of dimension 18, and τ acts on it with trace 0. On the whole cohomology, $\mathrm{Tr}(\tau) = 0$ because τ has no fixed points on the hypersurface (3) (for $u \neq 16$). As H^0 and H^4 contribute each 1 to the trace, the part of cohomology H^2 orthogonal to the 24 lines, as a representation, is

$1 \times$ [rectangle], $\tau = 1$ $\quad + \quad$ $3 \times$ [rectangle], $\tau = -1$.

over $\mathbb{C}$, must be of type $(1,1)$, hence algebraic — by specialization, same over $\overline{\mathbb{F}}_q$

over $\mathbb{C}$, Hodge type $(2,0)$ $(1,1)$ $(0,2)$ each of dim 1

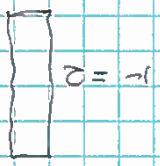
To count points of (3) over $\mathbb{F}_q$, one then needs to know the eigenvalues of Frobenius :

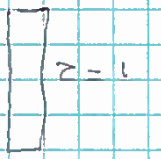
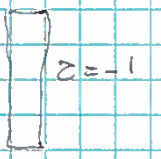
On the span of the 24 lines : $\mathrm{Frob} = q$

On the class in [rectangle], $\tau = 1$, perpendicular to this span : $\mathrm{Frob} = \pm q$

On the remaining orthogonal, we only know it is an orthogonal similitude with $< >$ multiplied by q^2 : if $\underset{q \cdot 50}{\text{in}}$: q, α, β with $|\alpha| = |\beta| = q$, $\alpha\beta = q^2$

if $\underset{q \cdot (0-50)}{\text{in}}$: $-q, \alpha, \beta$ with $|\alpha| = |\beta| = q$, $\alpha\beta = q^2$

For $u = 16$, one loses one  $z = -1$

For $u = -4$, " " one  $z = 1$ and one  $z = -1$

If V is the orthogonal, in H^2, of the span of the 24 lines (dimension 4), we eventually obtain

$$\#\text{ points of (1) over } \mathbb{F}_q = q^2 + \underbrace{\tau(\mathrm{Frob}, V)}_{|\ | \leq 4q} + 7$$

(when V drops to dimension 3 for $u = 16$, to dimension 2 for $u = -4$)

Bart

P. 7/