

Supercharacters and Mixed Moments of Kloosterman Sums

Ángel Chávez

Department of Mathematics, Pomona College, 610 N. College Ave.

Claremont, CA 91711

Angel.Chavez@pomona.edu

George Todd

Department of Mathematics, Union College, Bailey Hall 202

Schenectady, NY 12308

toddg@union.edu

Recent work has realized Kloosterman sums as supercharacter values of a supercharacter theory on $(\mathbb{F}_p)^2$. We use this realization to express fourth degree mixed power moments of Kloosterman sums in terms of the trace of Frobenius of a certain elliptic curve.

Keywords: supercharacters, kloosterman sums

1. Introduction

Supercharacters were introduced by Diaconis and Isaacs in 2008 [6] as a generalization of André's basic characters [1,2,3]. Recent work has expressed many exponential sums as values of various supercharacter theories arising from the action of subgroups of $\mathrm{GL}_d(\mathbb{Z}/n\mathbb{Z})$ on $(\mathbb{Z}/n\mathbb{Z})^d$ [4,5,9,10,11]. We investigate the supercharacter theory in [4] arising from the action of $\mathrm{GL}_2(\mathbb{F}_p)$ on $(\mathbb{F}_p)^2$ whose values correspond to Kloosterman sums. We then use the resulting supercharacter table and a result of Williams [20] to express fourth degree mixed Kloosterman moments in terms of the trace of Frobenius of an elliptic curve.

Fix a prime p . To each $a \in \mathbb{F}_p$ there corresponds an additive character ψ_a of \mathbb{F}_p

defined by

$$\psi_a(t) = e\left(\frac{at}{p}\right), \quad (1.1)$$

where $e(x) = \exp(2\pi ix)$. The *Kloosterman sum* corresponding to the additive characters ψ_a and ψ_b is the character sum defined by

$$K(\psi_a, \psi_b) = \sum_{t \in (\mathbb{F}_p)^\times} \psi_a(t) \psi_b(t^{-1}). \quad (1.2)$$

Define $K(a) = K(\psi_a, \psi_1)$. Then we call

$$V_n(p) = \sum_{t \in (\mathbb{F}_p)^\times} K(t)^n \quad (1.3)$$

the *n*th power moment of Kloosterman sums. Elementary methods in automorphic forms [14,18] are used to derive the following:

$$V_1(p) = 1, \quad (1.4)$$

$$V_2(p) = p^2 - p - 1, \quad (1.5)$$

$$V_3(p) = \left(\frac{p}{3}\right) p^2 + 2p + 1, \quad (1.6)$$

$$V_4(p) = 2p^3 - 3p^2 - 3p - 1, \quad (1.7)$$

where $(-)$ in (1.6) is the Legendre symbol. For $V_5(p)$, it can be shown [16,17] that

$$V_5(p) = \left(\frac{p}{3}\right) 4p^3 + (c_p + 5)p^2 + 4p + 1$$

for $p > 5$, where c_p is an integer with $|c_p| < 2p$. Moreover, [12] shows that $V_6(p)$ for $p > 7$ is given by

$$V_6(p) = 5p^4 - 10p^3 - (b_p + 9)p^2 - 5p - 1,$$

where b_p is the integer with $|b_p| < 2p^{3/2}$ defined as the p -th Fourier coefficient in the Fourier expansion of the newform of weight 4, level 6 given by $(\eta(z)\eta(2z)\eta(3z)\eta(6z))^2$, where η is the Dedekind eta function. Evans [7,8] conjectured and provided substantial numerical evidence for an evaluation of $V_7(p)$ in terms of Hecke eigenvalues of a weight-3 newform of $\Gamma_0(525)$ with quartic nebentypus of conductor 105, as well as a conjecture for an evaluation of $V_8(p)$ in terms of

Hecke eigenvalues of a weight-6 newform on $\Gamma_0(6)$ with trivial nebentypus. These conjectures were proved by Yun [21].

Kutzko derived the following in [15]:

$$\sum_{t \in (\mathbb{F}_p)^\times} K(t)K(at)K(bt) = \left(\frac{\beta(1, a, b)}{p} \right) p^2 + 2p, \quad (1.8)$$

where $\beta(i, j, k) = i^2 + j^2 + k^2 - 2ij - 2jk - 2ik$. This identity was rederived using supercharacters in [4,9]. Our main result concerns the *fourth-degree mixed moments*,

$$\sum_{t \in (\mathbb{F}_p)^\times} K(t)K(at)K(bt)K(ct),$$

where $a, b, c \in (\mathbb{F}_p)^\times$. We use the machinery developed in [4,9] to show

$$\sum_{t \in (\mathbb{F}_p)^\times} K(t)K(at)K(bt)K(ct) = \delta_{a,1}\delta_{b,c}p^3 - (\phi(bc)a_p + 2)p^2 - 3p - 1, \quad (1.9)$$

where ϕ is the Legendre character and a_p is the trace of Frobenius of the elliptic curve

$$y^2 = x \left(x^2 + \frac{\Delta}{16bc}x + \frac{a}{bc} \right)$$

over \mathbb{F}_q with $\Delta = 4(b-c)^2 - 8(a+1)(b+c) + 4(a-1)^2$, provided that $a, b, c \in (\mathbb{F}_p)^\times$ such that if $b+c \equiv a+1 \pmod{p}$, then $(b-c)^2 \not\equiv (a-1)^2 \pmod{p}$. We also require that $t^2 - 2(a+1)t + (a-1)^2$ and $t^2 - 2(b+c)t + (b-c)^2$ have no common root modulo p .

In Section 2, we give a brief overview of the supercharacter theory of [4], while slightly extending the underlying group to $G = R^r$, where $r \geq 1$ is a positive integer and R is a finite commutative ring with identity. Our main theorem is proved in Section 3.

2. Supercharacter Theories on $G = R^r$

This section provides a brief background on supercharacter theories and primarily follows [4].

Definition 2.1 (Diaconis-Isaacs [6]). *Let G be a finite group, \mathcal{X} a partition of the set $\text{Irr } G$ of irreducible characters of G , and let \mathcal{Y} a partition of G . The ordered*

pair $(\mathcal{X}, \mathcal{Y})$ is a supercharacter theory if the following conditions are satisfied:

(i) \mathcal{Y} contains $\{0\}$, where 0 is the identity in G .

(ii) $|\mathcal{X}| = |\mathcal{Y}|$.

(iii) For every $X \in \mathcal{X}$, the character $\sigma_X = \sum_{\psi \in X} \psi(0)\psi$ is constant on each $Y \in \mathcal{Y}$.

The characters σ_X are called supercharacters and the elements of \mathcal{Y} are called superclasses.

Our goal is to describe a certain class of supercharacter theories on $G = R^r$, where $r \geq 1$ is a positive integer and R is a finite commutative ring with multiplicative identity $1 \equiv 1_R$. The technique presented here depends on a choice of subgroup Γ of the group $\mathrm{GL}_r(R)$ of invertible $r \times r$ matrices with entries in R . We remark that this technique, in a slightly different context, was first described in [4].

Being a finite abelian group, R is isomorphic to the group \widehat{R} of additive characters of R . For each $\psi \in \widehat{R}$, we let ψ_x denote the image of x under a fixed isomorphism $R \rightarrow \widehat{R}$. An element $\psi \in \widehat{R}$ is called a *generating character* if $\psi_x(y) = \psi(xy)$ for all characters $\psi_x \in \widehat{R}$. Throughout this section, we assume R has a generating character ψ . It turns out that such a generating character ψ induces a natural generating character Ψ on G , which is defined by setting

$$\Psi(x_1, x_2, \dots, x_d) = \psi(x_1)\psi(x_2) \cdots \psi(x_d) \quad (2.1)$$

for each tuple $(x_1, x_2, \dots, x_d) \in G$. We remark that for each pair of elements $\mathbf{x} = (x_1, x_2, \dots, x_d)$ and $\mathbf{y} = (y_1, y_2, \dots, y_d)$, we have

$$\Psi_{\mathbf{x}}(\mathbf{y}) = \Psi(\mathbf{xy}) = \psi(\mathbf{x} \cdot \mathbf{y}), \quad (2.2)$$

where $\mathbf{x} \cdot \mathbf{y} = x_1y_1 + x_2y_2 + \cdots + x_dy_d$ and $\mathbf{xy} = (x_1y_1, x_2y_2, \dots, x_dy_d)$.

We let Γ be a subgroup $\mathrm{GL}_r(R)$ that is invariant under the transpose operation.

The subgroup Γ acts on \widehat{G} by $\Psi_{\mathbf{x}}^A = \Psi_{A^{-T}\mathbf{x}}$ where A^{-T} denotes the inverse transpose of A . Note that this defines a group action since $\Psi_{\mathbf{x}}^{AB} = (\Psi_{\mathbf{x}}^B)^A$. We will let \mathcal{X} denote the corresponding set of orbits in \widehat{G} . In addition, we let \mathcal{Y} denote the set of orbits in G induced by the action of Γ on G given by left multiplication: $(A, \mathbf{y}) \mapsto \mathbf{y}^A = A\mathbf{y}$. One has $\Psi_{\mathbf{x}}^A(\mathbf{y}^A) = \Psi_{\mathbf{x}}(\mathbf{y})$. A result of Brauer ([13], Thm. 6.3.2, Cor. 6.33) implies that \mathcal{X} and \mathcal{Y} contain the same number of orbits. Consequently, one defines

$$N = |\mathcal{X}| = |\mathcal{Y}|. \quad (2.3)$$

We will identify each character $\Psi_{\mathbf{x}} \in \widehat{G}$ with the corresponding element $\mathbf{x} \in G$ so that each orbit $X \in \mathcal{X}$ is stable under the action of Γ given by $(A, \mathbf{x}) \mapsto A^{-T}\mathbf{x}$. With this convention, we define a character σ_X corresponding to the orbit $X \in \mathcal{X}$ by setting

$$\sigma_X(\mathbf{y}) = \sum_{\mathbf{x} \in X} \Psi_{\mathbf{x}}(\mathbf{y}) = \sum_{\mathbf{x} \in X} \psi(\mathbf{x} \cdot \mathbf{y}). \quad (2.4)$$

These characters are class functions. In fact, if $\mathbf{y}' = A\mathbf{y}$ for some $A \in \Gamma$, then

$$\sigma_X(\mathbf{y}') = \sum_{\mathbf{x} \in X} \psi(\mathbf{x} \cdot A\mathbf{y}) = \sum_{\mathbf{x} \in X} \psi(A^T\mathbf{x} \cdot \mathbf{y}) = \sum_{\mathbf{x}' \in X} \psi(\mathbf{x}' \cdot \mathbf{y}) = \sigma_X(\mathbf{y}). \quad (2.5)$$

The fact that \mathcal{Y} contains the trivial orbit, together with (2.3) and (2.5), imply that the pair $(\mathcal{X}, \mathcal{Y})$ is a supercharacter theory on G .

Lastly, we identify any set X in \mathcal{X} with the set of vectors $\{\mathbf{x} : \psi_{\mathbf{x}} \in X\}$. With this identification, we have $\mathcal{X} = \mathcal{Y}$. We will therefore continue the convention in [4] and regard the elements of \mathcal{X} as *superclasses*. If Y is a superclass and $\mathbf{y} \in Y$, then we often write $\sigma_X(Y)$ in place of $\sigma_X(\mathbf{y})$ since σ_X is constant on superclasses.

We now give an overview of important results from [4], which hold in this slightly new context. We refer the reader to [4] for detailed proofs. To begin, we let $L^2(G)$ denote the set of complex-valued functions on G , which is endowed with the inner product

$$\langle f, g \rangle = \sum_{\mathbf{x} \in G} f(\mathbf{x})\overline{g(\mathbf{x})}. \quad (2.6)$$

Fix an enumeration X_1, X_2, \dots, X_N of $\mathcal{X} = \mathcal{Y}$ and let $\sigma_1, \sigma_2, \dots, \sigma_N$ denote the corresponding supercharacters. The irreducible characters (1.1) form an orthogonal set with respect to $\langle \cdot, \cdot \rangle$, which implies

$$\langle \sigma_i, \sigma_j \rangle = \delta_{i,j} \sum_{\mathbf{x} \in X_i} \langle \psi_{\mathbf{x}}, \psi_{\mathbf{x}} \rangle = |R|^r |X_i| \delta_{i,j}. \quad (2.7)$$

On the other hand,

$$\langle \sigma_i, \sigma_j \rangle = \sum_{\mathbf{x} \in G} \sigma_i(\mathbf{x}) \overline{\sigma_j(\mathbf{x})} = \sum_{\ell=1}^N |X_\ell| \sigma_i(X_\ell) \overline{\sigma_j(X_\ell)} \quad (2.8)$$

since the supercharacters are class functions. In particular, (2.7) and (2.8) together imply the unitarity of

$$U = \frac{1}{\sqrt{|R|^r}} \left[\frac{\sigma_i(X_j) \sqrt{|X_j|}}{\sqrt{|X_i|}} \right]_{i,j=1}^N. \quad (2.9)$$

Lemma 2.2 ([4], Lemma 1). *The unitary matrix given in (2.9) satisfies the following.*

(a) $U = U^T$

(b) $U^2 = P$, where P denotes the permutation matrix that interchanges positions i and j whenever $X_i = -X_j$ and fixes position i whenever $X_i = -X_i$.

(c) $U^4 = I$.

Theorem 2.3 ([4], Theorem 2). *Let R and Γ be as above. In addition, let $\sigma_1, \dots, \sigma_N$ denote the supercharacters corresponding to the superclasses X_1, \dots, X_N . For each fixed element $\mathbf{z} \in X_k$, we let $A_{i,j,k}$ denote the number of solutions $(\mathbf{x}_i, \mathbf{y}_j) \in X_i \times X_j$ to the equation $\mathbf{x} + \mathbf{y} = \mathbf{z}$.*

(a) $A_{i,j,k}$ is independent of the representative \mathbf{z} in X_k which is chosen

(b) The identity $\sigma_i(X_\ell)\sigma_j(X_\ell) = \sum_{k=1}^N A_{i,j,k}\sigma_k(X_\ell)$ holds for $1 \leq i, j, k, \ell \leq N$.

(c) The matrices T_1, \dots, T_N , whose entries are given by

$$[T_i]_{j,k} = \frac{A_{i,j,k}\sqrt{|X_k|}}{\sqrt{|X_j|}}$$

each satisfy $T_i U = U D_i$, where $D_i = \text{diag}(\sigma_i(X_1), \sigma_i(X_2), \dots, \sigma_i(X_N))$.

(d) Each matrix T_i is normal and the set $\{T_1, \dots, T_N\}$ forms a basis for the algebra \mathcal{A} of all $N \times N$ matrices T such that $U^* T U$ is diagonal.

We now take $R = \mathbb{F}_q$. In this case, R has generating character ψ defined by

$$\psi(\alpha) = e\left(\frac{\text{tr}(\alpha)}{p}\right). \quad (2.10)$$

If $q = p$, then the field trace $\text{tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p$ is the identity map and (2.4) reduces to the supercharacters as seen in [4]. Arising in this way are several interesting exponential sums from number theory (e.g. Gauss, Kloosterman, Heilbronn, etc.) to which we refer the reader [4,5,9,10,11]. In this paper, we focus on a rather simple supercharacter theory on $(\mathbb{F}_q)^2$.

Example 2.4 (Kloosterman Sums).

Let $r = 2$. Consider the symmetric subgroup

$$\Gamma = \left\{ \begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix} : x \in (\mathbb{F}_q)^\times \right\}$$

of $\text{GL}_2(\mathbb{F}_q)$. There are $p - 1$ non-trivial Γ -orbits in $(\mathbb{F}_q)^2$ defined by

$$X(a) = \{(at, t^{-1}) : t \in (\mathbb{F}_q)^\times\} \quad (a \in (\mathbb{F}_q)^\times).$$

In addition, there are *trivial* orbits $X_1 = \{(a, 0) : a \in (\mathbb{F}_q)^\times\}$, $X_2 = \{(0, a) : a \in (\mathbb{F}_q)^\times\}$ and $X_3 = \{(0, 0)\}$. If $a, b \in (\mathbb{F}_q)^\times$, then

$$\begin{aligned} \sigma_{X(a)}(X(b)) &= \sum_{t \in (\mathbb{F}_q)^\times} e\left(\frac{\text{tr}[(tab + t^{-1})]}{p}\right) \\ &= K(\psi_{ab}, \psi_1). \end{aligned}$$

3. Fourth-Degree Sums

We continue to work with the supercharacter theory of Example 2.4. However, we will agree to work over \mathbb{F}_p in order to simplify notation. We observe that D_i is the diagonal matrix

$$\text{diag}\left(\sigma_i(X(1)), \sigma_i(X(2)), \dots, \sigma_{X_i}(X(p-1)), \sigma_{X_i}(X_1), \dots, \sigma_{X_i}(X_3)\right),$$

where the entries are given in Example 2.4. In particular, if $1 \leq i \leq p-1$, then

$$D_i = \text{diag}\left(K(i), K(2i), \dots, K((p-1)i), -1, -1, p-1\right). \quad (3.1)$$

In addition,

$$U = q^{-1} \left[\begin{array}{cccc|ccc} K(1) & K(2) & \cdots & K(p-1) & -1 & -1 & \sqrt{p-1} \\ K(2) & K(4) & \cdots & K(2(p-1)) & -1 & -1 & \sqrt{p-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ K(p-1) & K(2(p-1)) & \cdots & K((p-1)^2) & -1 & -1 & \sqrt{p-1} \\ \hline -1 & -1 & \cdots & -1 & -1 & p-1 & \sqrt{p-1} \\ -1 & -1 & \cdots & -1 & p-1 & -1 & \sqrt{p-1} \\ \sqrt{p-1} & \sqrt{p-1} & \cdots & \sqrt{p-1} & \sqrt{p-1} & \sqrt{p-1} & 1 \end{array} \right].$$

Begin by fixing $c \in (\mathbb{F}_p)^\times$. The integer $A_{a,b,c}$ denotes the number of solutions $(\mathbf{x}_a, \mathbf{y}_b) \in X(a) \times X(b)$ to the equation $\mathbf{x}_a + \mathbf{y}_b = (c, 1)$, which by Example 2.4 is equivalent to

$$\begin{aligned} at + bs &= c, \\ t^{-1} + s^{-1} &= 1. \end{aligned}$$

Note that we necessarily have $t \neq 1$. Solving for s in the second equation and substituting into the first equation implies

$$at^2 + (b-a-c)t + c = 0. \quad (3.2)$$

Therefore,

$$A_{a,b,c} = 1 + \phi(\beta(a, b, c)), \quad (3.3)$$

where

$$\beta(i, j, k) = i^2 + j^2 + k^2 - 2ij - 2ik - 2jk \quad (3.4)$$

is the discriminant of quadratic (3.2). An important observation is that $\beta(a, b, c)$ is invariant under permutations. The entries (3.3) account for the upper-left $(p-1) \times (p-1)$ block of T_a . In particular, we have

$$T_a = \left[\begin{array}{cccccc|ccc} A_{a,1,1} & A_{a,1,2} & \cdots & A_{a,1,a} & \cdots & A_{a,1,p-1} & 1 & 1 & 0 \\ A_{a,2,1} & A_{a,2,2} & \cdots & A_{a,2,a} & \cdots & A_{a,2,p-1} & 1 & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ A_{a,a,1} & A_{a,a,2} & \cdots & A_{a,a,a} & \cdots & A_{a,a,p-1} & 0 & 0 & \sqrt{p-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \hline A_{a,p-1,1} & A_{a,p-1,2} & \cdots & A_{a,p-1,a} & \cdots & A_{a,p-1,p-1} & 1 & 1 & 0 \\ \hline 1 & 1 & \cdots & 0 & \cdots & 1 & 0 & 1 & 0 \\ 1 & 1 & \cdots & 0 & \cdots & 1 & 1 & 0 & 0 \\ 0 & 0 & \cdots & \sqrt{p-1} & \cdots & 0 & 0 & 0 & 0 \end{array} \right].$$

One may verify that if $a, b, c \in (\mathbb{F}_p)^\times$, then

$$[T_a T_b]_{1,c} = \rho(a, b, c) + 2(1 - \delta_{a,1})(1 - \delta_{b,c}) + (p-1)\delta_{a,1}\delta_{b,c}, \quad (3.5)$$

where $\delta_{i,j}$ denotes the delta function and

$$\rho(a, b, c) = \sum_{\ell=1}^{p-1} A_{a,1,\ell} A_{b,c,\ell}. \quad (3.6)$$

One readily verifies the following.

Lemma 3.1. *Suppose $a, b \in (\mathbb{F}_p)^\times$. Then*

$$\sum_{t \in (\mathbb{F}_p)^\times} A_{a,b,t} = p - 3 + \delta_{a,b}. \quad (3.7)$$

Lemma 3.2. *Let $a_1, a_2, \dots, a_{n-1} \in (\mathbb{F}_p)^\times$ and denote $\lambda = p - 1$.*

(a) *If $a_n \in (\mathbb{F}_p)^\times$, then*

$$\sum_{t \in (\mathbb{F}_p)^\times} K(t)K(a_1 t)K(a_2 t) \cdots K(a_n t) = p^2 \left[T_{a_1} T_{a_2} \cdots T_{a_{n-1}} \right]_{1,a_n} + 2(-1)^n - \lambda^n.$$

(b) If $a_n = p, p + 1$, then

$$\sum_{t \in (\mathbb{F}_p)^\times} K(t)K(a_1t)K(a_2t) \cdots K(a_{n-1}t) = -p^2 \left[T_{a_1} T_{a_2} \cdots T_{a_{n-1}} \right]_{1, a_n} + \lambda^n + (-1)^n \lambda + (-1)^{n+1}$$

(c) If $a_n = p + 2$, then

$$\sum_{t \in (\mathbb{F}_p)^\times} K(t)K(a_1t)K(a_2t) \cdots K(a_{n-1}t) = p^2 \lambda^{-1/2} \left[T_{a_1} T_{a_2} \cdots T_{a_{n-1}} \right]_{1, a_n} + 2(-1)^{n+1} - \lambda^{n-1}.$$

Proof. Each formula comes from comparing the $(1, a_n)$ -entry of the matrix $UD_{a_1}D_{a_2} \cdots D_{a_{n-1}}U^*$ with the $(1, a_n)$ -entry of $T_{a_1}T_{a_2} \cdots T_{a_{n-1}}$. For brevity, we denote $\lambda = p - 1$. Noting that U is real-valued, one can compute the a_n^{th} column of $D_{a_1}D_{a_2} \cdots D_{a_{n-1}}U^*$ by taking an entry-wise product of the vector

$$\left[K(a_1) \cdots K(a_{n-1}), \dots, K(\lambda a_1) \cdots K(\lambda a_{n-1}), (-1)^{n-1}, (-1)^{n-1}, \lambda^{n-1} \right]$$

with the a_n^{th} row of U . The identities follow. \square

This gives us the following identities for the n -th power moment of Kloosterman sums.

Corollary 3.3.

$$V_n(p) = p^2 [T_1]_{1,1}^{n-2} + 2(-1)^{n-1} - (p-1)^{n-1}$$

We use Lemma 3.2 to derive a closed-form for mixed fourth-degree moments. First, we recall a result of Williams [19,20]:

$$\sum_t F\left((at^2 + bt + c)(At^2 + Bt + C)^{-1}\right) = \sum_t F(t) + \sum_t F(t)\phi\left(Dx^2 + \Delta t + D'\right) - F(a/A), \quad (3.8)$$

where F is any p -periodic complex-valued function defined on \mathbb{Z} and $A, B, C, a, b, c \in \mathbb{Z}$ such that $A \not\equiv 0 \pmod{p}$ and $\Delta^2 - 4DD' \not\equiv 0 \pmod{p}$, and if $aB - bA \equiv 0 \pmod{p}$ then $aC - cA \not\equiv 0 \pmod{p}$. We also require that $at^2 + bt + c$ and $At^2 + Bt + C$ do not have a common root modulo p . Here, we have defined

$$D = B^2 - 4AC, \quad \Delta = 4aC - 2Bb + 4cA, \quad D' = b^2 - 4ac. \quad (3.9)$$

We remark that $(\cdot)^{-1}$ denotes the inverse modulo p and also that the sums appearing in (3.8) are taken over \mathbb{F}_p .

Theorem 3.4. *Suppose $a, b, c \in (\mathbb{F}_p)^\times$ such that if $b + c \equiv a + 1 \pmod{p}$, then $(b - c)^2 \not\equiv (a - 1)^2 \pmod{p}$. We also require that $t^2 - 2(a + 1)t + (a - 1)^2$ and $t^2 - 2(b + c)t + (b - c)^2$ have no common root modulo p . Then*

$$\sum_{t \in (\mathbb{F}_p)^\times} K(t)K(at)K(bt)K(ct) = \delta_{a,1}\delta_{b,c}p^3 - \left(\phi(bc)a_p + 2\right)p^2 - 3p - 1, \quad (3.10)$$

where a_p is the trace of Frobenius of the elliptic curve

$$y^2 = x\left(x^2 + \frac{\Delta}{16bc}t + \frac{a}{bc}\right)$$

over \mathbb{F}_p with $\Delta = 4(b - c)^2 - 8(a + 1)(b + c) + 4(a - 1)^2$.

Proof. By Lemma 3.2, it remains only to simplify expression (3.5). To this end, we observe

$$\rho(a, b, c) = p - 1 + \sum_{t \in (\mathbb{F}_p)^\times} \left[\phi(\beta(a, 1, t)) + \phi(\beta(b, c, t)) \right] + \sum_{t \in (\mathbb{F}_p)^\times} \phi(\beta(a, 1, t)\beta(b, c, t)). \quad (3.11)$$

Using the following elementary result

$$\sum_{t \in \mathbb{F}_p} \phi(At^2 + Bt + C) = \begin{cases} (p - 1)\phi(A) & B^2 - 4AC = 0 \\ -\phi(A) & B^2 - 4AC \neq 0, \end{cases} \quad (3.12)$$

we have

$$\sum_{t \in \mathbb{F}_p} \phi(\beta(a, 1, t)) = \begin{cases} (p - 1)\phi(1) & 16a = 0 \\ -\phi(1) & 16a \neq 0. \end{cases} \quad (3.13)$$

Since p is odd and $a \neq 0$, we have $16a \neq 0$. This implies

$$\sum_{t \in (\mathbb{F}_p)^\times} \phi(\beta(a, 1, t)) = -1 - \phi((a - 1)^2) = -2 + \delta_{a,1}.$$

Similarly, we observe that $\beta(b, c, t) = t^2 - 2(b + c)t + (b - c)^2$, and we obtain

$$\sum_{t \in (\mathbb{F}_p)^\times} \phi(\beta(b, c, t)) = -2 + \delta_{b,c}.$$

Taking $F = \phi$ in (3.8) implies

$$\begin{aligned} \sum_{t \in (\mathbb{F}_p)} \phi\left(\beta(a, 1, t)\beta(b, c, t)\right) &= \sum_{t \in (\mathbb{F}_p)} \phi\left((t^2 - 2(a+1)t + (a-1)^2)(t^2 - 2(b+c)t + (b-c)^2)\right) \\ &= -1 + \sum_{t \in (\mathbb{F}_p)^\times} \phi(Dt^3 + \Delta t^2 + D't), \end{aligned}$$

which gives that

$$\begin{aligned} \sum_{t \in (\mathbb{F}_p)^\times} \phi\left(\beta(a, 1, t)\beta(b, c, t)\right) &= -1 + \sum_{t \in (\mathbb{F}_p)^\times} \phi(Dt^3 + \Delta t^2 + D't) - \phi(\beta(a, 1, 0)\beta(b, c, 0)) \\ &= -1 + \sum_{t \in (\mathbb{F}_p)^\times} \phi(Dt^3 + \Delta t^2 + D't) - (1 - \delta_{a,1})(1 - \delta_{b,c}) \end{aligned}$$

provided that if $b + c \equiv a + 1 \pmod{p}$ then $(b - c)^2 \not\equiv (a - 1)^2 \pmod{p}$, the two quadratics share no roots modulo p , and where $D = 16bc$, $D' = 16a$, and $\Delta = 4(b - c)^2 - 8(a + 1)(b + c) + 4(a - 1)^2$. This completes the proof. \square

4. Acknowledgements

The authors wish to thank Stephan Ramon Garcia for helpful discussions and feedback. We also wish to thank the referees for helpful suggestions, as well as for drawing our attention to the apparent asymmetry in (1.9). That this is symmetric in a , b , and c under the given hypotheses follows from Theorem 3.4, but an independent explanation would be interesting.

References

- [1] Carlos A. M. André. Basic characters of the unitriangular group. *J. Algebra*, 175(1):287–319, 1995.
- [2] Carlos A. M. André. The basic character table of the unitriangular group. *J. Algebra*, 241(1):437–471, 2001.
- [3] Carlos A. M. André. Basic characters of the unitriangular group (for arbitrary primes). *Proc. Amer. Math. Soc.*, 130(7):1943–1954, 2002.
- [4] J. L. Brumbaugh, Madeleine Bulkow, Patrick S. Fleming, Luis Alberto Garcia German, Stephan Ramon Garcia, Gizem Karaali, Matt Michal, Andrew P. Turner, and Hong Suh. Supercharacters, exponential sums, and the uncertainty principle. *J. Number Theory*, 144:151–175, 2014.

- [5] J. L. Brumbaugh, Madeleine Bulkow, Luis Alberto Garcia German, Stephan Ramon Garcia, Matt Michal, and Andrew P. Turner. The graphic nature of the symmetric group. *Exp. Math.*, 22(4):421–442, 2013.
- [6] Persi Diaconis and I. M. Isaacs. Supercharacters and superclasses for algebra groups. *Trans. Amer. Math. Soc.*, 360(5):2359–2392, 2008.
- [7] Ron Evans. Hypergeometric (1/4) evaluations over finite fields and Hecke eigenforms. *Proc. Amer. Math. Soc.*, 138(2):517–531, 2010.
- [8] Ronald Evans. Seventh power moments of Kloosterman sums. *Israel J. Math.*, 175:349–362, 2010.
- [9] Patrick S. Fleming, Stephan Ramon Garcia, and Gizem Karaali. Classical Kloosterman sums: representation theory, magic squares, and Ramanujan multigraphs. *J. Number Theory*, 131(4):661–680, 2011.
- [10] Christopher F. Fowler, Stephan Ramon Garcia, and Gizem Karaali. Ramanujan sums as supercharacters. *Ramanujan J.*, 35(2):205–241, 2014.
- [11] Stephan Ramon Garcia, Trevor Hyde, and Bob Lutz. Gauss’s hidden menagerie: from cyclotomy to supercharacters. *Notices Amer. Math. Soc.*, 62(8):878–888, 2015.
- [12] K. Hulek, J. Spandaw, B. van Geemen, and D. van Straten. The modularity of the Barth-Nieto quintic and its relatives. *Adv. Geom.*, 1(3):263–289, 2001.
- [13] I. Martin Isaacs. *Character theory of finite groups*. AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423].
- [14] Henryk Iwaniec. *Topics in classical automorphic forms*, volume 17 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1997.
- [15] Philip C. Kutzko. The cyclotomy of finite commutative P.I.R.’s. *Illinois J. Math.*, 19:1–17, 1975.
- [16] Ron Livné. Motivic orthogonal two-dimensional representations of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Israel J. Math.*, 92(1-3):149–156, 1995.
- [17] C. Peters, J. Top, and M. van der Vlugt. The Hasse zeta function of a $K3$ surface related to the number of words of weight 5 in the Melas codes. *J. Reine Angew. Math.*, 432:151–176, 1992.
- [18] Hans Salié. über die Kloostermanschen Summen $S(u, v; q)$. *Math. Z.*, 34(1):91–109, 1932.
- [19] Kenneth S. Williams. Finite transformation formulae involving the Legendre symbol. *Pacific J. Math.*, 34:559–568, 1970.

- [20] Kenneth S. Williams. Evaluation of character sums connected with elliptic curves. *Proc. Amer. Math. Soc.*, 73(3):291–299, 1979.
- [21] Zhiwei Yun. Galois representations attached to moments of Kloosterman sums and conjectures of Evans. *Compos. Math.*, 151(1):68–120, 2015. Appendix B by Christelle Vincent.