1-1-2011

Classical Kloosterman Sums: Representation Theory, Magic Squares, and Ramanujan Multigraphs

Patrick S. Fleming
South Dakota School of Mines and Technology

Stephan Ramon Garcia
Pomona College

Gizem Karaali
Pomona College

Recommended Citation

Patrick S. Fleming, Stephan Ramon Garcia, Gizem Karaali, Classical Kloosterman sums: Representation theory, magic squares, and Ramanujan multigraphs, Journal of Number Theory, Volume 131, Issue 4, April 2011, Pages 661-680, ISSN 0022-314X, 10.1016/j.jnt.2010.10.009. (http://www.sciencedirect.com/science/article/pii/S0022314X10002684)

CLASSICAL KLOOSTERMAN SUMS: REPRESENTATION THEORY, MAGIC SQUARES, AND RAMANUJAN MULTIGRAPHS

PATRICK S. FLEMING, STEPHAN RAMON GARCIA, AND GIZEM KARAALI

Abstract. We consider a certain finite group for which Kloosterman sums appear as character values. This leads us to consider a concrete family of commuting hermitian matrices which have Kloosterman sums as eigenvalues. These matrices satisfy a number of "magical" combinatorial properties and they encode various arithmetic properties of Kloosterman sums. These matrices can also be regarded as adjacency matrices for multigraphs which display Ramanujan-like behavior.

1. Introduction

For a fixed odd prime p, let $\zeta = \exp(2\pi i/p)$ and define the classical *Kloosterman sum* $K(a,b) := K(a,b,p)$ by setting

$$K(a,b) = \sum_{n=1}^{p-1} \zeta^{an+b\overline{n}} \tag{1.1}$$

where $\overline{n}$ denotes the inverse of n modulo p. From (1.1), it follows that $K(a,b)$ is real and that its value depends only upon the residue classes of a and b modulo p. In light of the fact that $K(a,b) = K(1,ab)$ whenever $p \nmid a$, we focus our attention mostly on Kloosterman sums of the form $K(1,u)$. Moreover, we adopt the shorthand $K(u) := K(1,u)$ or even $K_u := K(1,u)$ when space is at a premium.

In the years since they appeared in Kloosterman's paper on quadratic forms [12], these exponential sums and their generalizations have found many diverse applications. We do not attempt to give a historical account of the subject and instead direct the reader to [5, 7, 9, 11].

In this note we construct a certain finite group for which Kloosterman sums appear as character values (Section 2). This eventually leads us to consider a concrete family of commuting hermitian matrices which have Kloosterman sums as eigenvalues (Section 3). These matrices satisfy a number of "magical" combinatorial properties (Section 4) and they encode various arithmetic properties of Kloosterman sums (Section 5). Moreover, these matrices can be regarded as the adjacency matrices for multigraphs which display Ramanujan-like behavior (Section 6).

Acknowledgments. We thank Philip C. Kutzko for suggesting the initial representation theory project that spurred this work. In particular, our basic approach stems from his paper [13]. We also thank the American Institute of Mathematics

This work partially funded by NSF grant DMS-0901523 (*Research Experiences for Undergraduate Faculty*). S.R. Garcia partially funded by NSF grants DMS-0638789 and DMS-1001614.

(AIM) for hosting us for a week as part of the NSF-funded (DMS-0901523) *Research Experiences for Undergraduate Faculty* program.

2. The group $\mathbf{G}$ and its representation theory

Let $p > 3$ be an odd prime and define the subgroup

$$\mathbf{G} = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} x^{-1} & z \\ 0 & 1 \end{pmatrix} \middle| \, x \in (\mathbb{Z}/p\mathbb{Z})^\times, \, y, z \in \mathbb{Z}/p\mathbb{Z} \right\}$$

of $GL_4(\mathbb{Z}/p\mathbb{Z})$. Here we identify direct sums of two 2×2 matrices with the corresponding 4×4 matrices. In the following, we denote matrix groups by bold capital letters (e.g., $\mathbf{G}$) and their elements by capital letters (e.g., I denotes the 4×4 identity matrix in $\mathbf{G}$). Elements of $\mathbb{Z}/p\mathbb{Z}$ are represented by lower-case letters.

Letting

$$\mathbf{N} = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \middle| \, y, z \in \mathbb{Z}/p\mathbb{Z} \right\}, \tag{2.1}$$

$$\mathbf{T} = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} x^{-1} & 0 \\ 0 & 1 \end{pmatrix} \middle| \, x \in (\mathbb{Z}/p\mathbb{Z})^\times \right\}, \tag{2.2}$$

we find that $\mathbf{G} = \mathbf{NT}$ and $\mathbf{N} \cap \mathbf{T} = \{I\}$. Since $|\mathbf{T}| = p - 1$ and $|\mathbf{N}| = p^2$, we have

$$|\mathbf{G}| = (p-1)p^2.$$

The conjugacy classes of $\mathbf{G}$ are easily computable and are given in Table 2.1.

Since the commutator subgroup $[\mathbf{G}, \mathbf{G}] = \mathbf{N}$ of $\mathbf{G}$ must belong to the kernel of any one-dimensional representation $\pi : \mathbf{G} \to \mathbb{C}$, it follows that $\pi(NT) = \pi(N)\pi(T) = \pi(T)$ for all $N \in \mathbf{N}$ and $T \in \mathbf{T}$. Thus the one-dimensional representations of $\mathbf{G}$ correspond to one-dimensional representations of $\mathbf{T} \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Fix a primitive $(p-1)$st root of unity ξ. If T denotes a generator of $\mathbf{T}$, then for $n = 1, 2, \ldots, p-1$ the formula

$$\pi(T) = \xi^n, \qquad \pi(N) = 1, \quad N \in \mathbf{N}$$

yields $p - 1$ distinct irreducible representation of $\mathbf{G}$.

Let us now identify the remaining irreducible representations. As before, we let $\zeta = \exp(2\pi i/p)$. Fixing $a, b \in \mathbb{Z}/p\mathbb{Z}$, at least one of which is nonzero, we claim that the map $\pi : \mathbf{G} \to \mathrm{End}(\mathbb{C}[(\mathbb{Z}/p\mathbb{Z})^\times])$ defined by

$$\pi\left(\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} x^{-1} & z \\ 0 & 1 \end{pmatrix} \right) \delta_h = \zeta^{az(xh) + by(xh)^{-1}} \delta_{xh} \tag{2.3}$$

for $h \in (\mathbb{Z}/p\mathbb{Z})^\times$ is an irreducible representation of $\mathbf{G}$. Verifying that π is a homomorphism is straightforward, so we only prove irreducibility.

Suppose that $a \neq 0$ and note that setting $x = 1$, $y = 0$, and $z = 1$ in (2.3) yields

$$\pi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right) \delta_h = \zeta^{ah} \delta_h$$

for $h \in (\mathbb{Z}/p\mathbb{Z})^\times$. The preceding is just another way of saying that

$$\pi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right) = \mathrm{diag}((\zeta^a)^1, (\zeta^a)^2, \ldots, (\zeta^a)^{p-1}) \tag{2.4}$$

with respect to the standard basis $\{\delta_1, \delta_2, \ldots, \delta_{p-1}\}$ of $\mathbb{C}[(\mathbb{Z}/p\mathbb{Z})^\times]$. Since $a \neq 0$ it follows that ζ^a is a primitive pth root of unity and hence the diagonal entries

TYPE 1: $p-1$ classes	$\mathcal{C}_1$	$=$	$\left\{\begin{pmatrix}1 & y\\ 0 & 1\end{pmatrix}\oplus\begin{pmatrix}1 & y^{-1}\\ 0 & 1\end{pmatrix} : y\in(\mathbb{Z}/p\mathbb{Z})^\times\right\}$	($p-1$ elements)
	$\mathcal{C}_2$	$=$	$\left\{\begin{pmatrix}1 & 2y\\ 0 & 1\end{pmatrix}\oplus\begin{pmatrix}1 & y^{-1}\\ 0 & 1\end{pmatrix} : y\in(\mathbb{Z}/p\mathbb{Z})^\times\right\}$	($p-1$ elements)
	$\vdots$		$\vdots$	$\vdots$
	$\mathcal{C}_{p-1}$	$=$	$\left\{\begin{pmatrix}1 & (p-1)y\\ 0 & 1\end{pmatrix}\oplus\begin{pmatrix}1 & y^{-1}\\ 0 & 1\end{pmatrix} : y\in(\mathbb{Z}/p\mathbb{Z})^\times\right\}$	($p-1$ elements)
TYPE 2: 2 classes	$\mathcal{C}_p$	$=$	$\left\{\begin{pmatrix}1 & y\\ 0 & 1\end{pmatrix}\oplus\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} : y\in(\mathbb{Z}/p\mathbb{Z})^\times\right\}$	($p-1$ elements)
	$\mathcal{C}_{p+1}$	$=$	$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\oplus\begin{pmatrix}1 & y\\ 0 & 1\end{pmatrix} : y\in(\mathbb{Z}/p\mathbb{Z})^\times\right\}$	($p-1$ elements)
TYPE 3: 1 class	$\mathcal{C}_{p+2}$	$=$	$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\oplus\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right\}$	(1 element)
TYPE 4: $p-2$ classes	$\mathcal{C}_{p+3}$	$=$	$\left\{\begin{pmatrix}g & y\\ 0 & 1\end{pmatrix}\oplus\begin{pmatrix}g^{-1} & z\\ 0 & 1\end{pmatrix} : y,z\in\mathbb{Z}/p\mathbb{Z}\right\}$	(p^2 elements)
	$\mathcal{C}_{p+4}$	$=$	$\left\{\begin{pmatrix}g^2 & y\\ 0 & 1\end{pmatrix}\oplus\begin{pmatrix}g^{-2} & z\\ 0 & 1\end{pmatrix} : y,z\in\mathbb{Z}/p\mathbb{Z}\right\}$	(p^2 elements)
	$\vdots$		$\vdots$	$\vdots$
	$\mathcal{C}_{2p}$	$=$	$\left\{\begin{pmatrix}g^{p-2} & y\\ 0 & 1\end{pmatrix}\oplus\begin{pmatrix}g^{-(p-2)} & z\\ 0 & 1\end{pmatrix} : y,z\in\mathbb{Z}/p\mathbb{Z}\right\}$	(p^2 elements)

TABLE 2.1. The conjugacy classes of $\mathbf{G}$ (here g denotes a primitive root modulo p). In particular, $\mathbf{G}$ has a total of $2p$ conjugacy classes whence there exist precisely $2p$ distinct irreducible representations of $\mathbf{G}$ [2, Theorem 27.22].

of (2.4) are distinct. Thus the subspaces of $\mathbb{C}[(\mathbb{Z}/p\mathbb{Z})^\times]$ which are invariant under the matrix (2.4) are precisely those of the form $\operatorname{span}(K)$ for some $K\subseteq(\mathbb{Z}/p\mathbb{Z})^\times$. Suppose that $K\neq\varnothing$, $K\neq(\mathbb{Z}/p\mathbb{Z})^\times$, and $x\notin K$. For each $k\in K$, (2.3) implies that

$$\pi\left(\begin{pmatrix}xk^{-1} & 0\\ 0 & 1\end{pmatrix}\oplus\begin{pmatrix}x^{-1}k & 0\\ 0 & 1\end{pmatrix}\right)\delta_k=\delta_{(xk^{-1})k}=\delta_x\notin\operatorname{span}(K).$$

Thus $\operatorname{span}(K)$ is not invariant under π whence π is irreducible, as claimed. The proof in the case $b\neq 0$ is similar.

The choices $a=1$, $b=0$ and $a=0$, $b=1$ lead us to two special characters, whose values on the various conjugacy classes can be found via a geometric series argument. We are interested primarily in π arising when $a\neq 0$ and $b\neq 0$. Let χ_j denote the trace of π corresponding to $j=a^{-1}b$. Using the transformation rules for Kloosterman sums we find that $\chi_j(\mathcal{C}_k)=K(a,bk)=K(1,jk)=K_{jk}$ for $1\leq j,k\leq p-1$. Since the Kloosterman sums $K(1),K(2),\ldots,K(p-1)$ are distinct [4, Prop. 1.3], it follows that the characters $\chi_1,\chi_2,\ldots,\chi_{p-1}$ are distinct. Now we can complete the character table for $\mathbf{G}$ (Table 2.2).

$\mathbf{G}$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\cdots$	$\mathcal{C}_{p-1}$	$\mathcal{C}_p$	$\mathcal{C}_{p+1}$	$\mathcal{C}_{p+2}$	$\mathcal{C}_{p+3}$	$\mathcal{C}_{p+4}$	$\cdots$	$\mathcal{C}_{2p}$
	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$ $\oplus$ $\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$ $\oplus$ $\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\cdots$ $\cdots$ $\cdots$	$\begin{pmatrix}1&f\\0&1\end{pmatrix}$ $\oplus$ $\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$ $\oplus$ $\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\oplus$ $\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\oplus$ $\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}g&0\\0&1\end{pmatrix}$ $\oplus$ $\begin{pmatrix}g^{-1}&0\\0&1\end{pmatrix}$	$\begin{pmatrix}g^2&0\\0&1\end{pmatrix}$ $\oplus$ $\begin{pmatrix}g^{-2}&0\\0&1\end{pmatrix}$	$\cdots$ $\cdots$ $\cdots$	$\begin{pmatrix}g^{p-2}&0\\0&1\end{pmatrix}$ $\oplus$ $\begin{pmatrix}g^{-(p-2)}&0\\0&1\end{pmatrix}$
$\lvert\mathcal{C}_i\rvert$	f	f	$\cdots$	f	f	f	1	p^2	p^2	$\cdots$	p^2
χ_1	K_1	K_2	$\cdots$	K_f	-1	-1	f	0	0	$\cdots$	0
χ_2	K_2	K_4	$\cdots$	K_{2f}	-1	-1	f	0	0	$\cdots$	0
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_{p-1}	K_f	K_{2f}	$\cdots$	K_{f^2}	-1	-1	f	0	0	$\cdots$	0
χ_p	-1	-1	$\cdots$	-1	f	-1	f	0	0	$\cdots$	0
χ_{p+1}	-1	-1	$\cdots$	-1	-1	f	f	0	0	$\cdots$	0
χ_{p+2}	1	1	$\cdots$	1	1	1	1	1	1	$\cdots$	1
χ_{p+3}	1	1	$\cdots$	1	1	1	1	ξ	ξ^2	$\cdots$	ξ^{p-2}
χ_{p+4}	1	1	$\cdots$	1	1	1	1	ξ^2	ξ^4	$\cdots$	$\xi^{2(p-2)}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_{2p}	1	1	$\cdots$	1	1	1	1	$\xi^{(p-2)}$	$\xi^{2(p-2)}$	$\cdots$	$\xi^{(p-2)^2}$

TABLE 2.2. The character table of $\mathbf{G}$. Here ξ is a fixed primitive $(p-1)$st root of unity and $f = p-1$. Since $K_0 = K_p = -1$, we may regard the initial string of -1's in the row corresponding to χ_p as being K_0's. This convention will simplify several formulas later on.

3. The main construction

3.1. **The crucial lemma.** From the representation-theoretic information computed in Section 2, we will construct a family of commuting hermitian matrices which encode many fundamental properties of classical Kloosterman sums. Our primary tool is the following lemma, which is a modification of [13, Lem. 4] (although there the reader is simply referred to [2, Section 33] to compose a proof of this lemma on their own). We provide a detailed proof for the sake of completeness.

Lemma 3.1. *Let $\mathbf{G}$ be a finite group having conjugacy classes $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_s$ and irreducible representations $\pi_1, \pi_2, \ldots, \pi_s$ with corresponding characters $\chi_1, \chi_2, \ldots, \chi_s$. For $1 \leq k \leq s$, fix $z = z(k) \in \mathcal{C}_k$ and let $c_{i,j,k}$ denote the number of solutions $(x_i, y_j) \in \mathcal{C}_i \times \mathcal{C}_j$ of $xy = z$ and then let $M_i = (c_{i,j,k})_{j,k=1}^s$ for $1 \leq i \leq s$.*

If $W = (w_{j,k})_{j,k=1}^s$ denotes the $s \times s$ matrix with entries

$$w_{j,k} = \frac{|\mathcal{C}_j| \chi_k(\mathcal{C}_j)}{\dim \pi_k}, \tag{3.1}$$

and $D_i = \operatorname{diag}(w_{i,1}, w_{i,2}, \ldots, w_{i,s})$, then W is invertible and

$$M_i W = W D_i \tag{3.2}$$

for $i = 1, 2, \ldots, s$. Moreover, if we let $Q = \operatorname{diag}(\sqrt{|\mathcal{C}_1|}, \sqrt{|\mathcal{C}_2|}, \ldots, \sqrt{|\mathcal{C}_s|})$, then the matrices $T_i = Q^{-1} M_i Q$ are simultaneously unitarily diagonalizable. To be more specific, we have $T_i U = U D_i$ for $i = 1, 2, \ldots, s$ where

$$U = \frac{1}{\sqrt{|\mathbf{G}|}} \left(\sqrt{|\mathcal{C}_j|} \chi_k(\mathcal{C}_j) \right)_{j,k=1}^s \tag{3.3}$$

is a unitary matrix.

Proof. For $j = 1, 2, \ldots, s$ define

$$\mathsf{C}_j = \sum_{x \in \mathcal{C}_j} x$$

and observe that

$$\mathsf{C}_i \mathsf{C}_j = \sum_{k=1}^s c_{i,j,k} \mathsf{C}_k \tag{3.4}$$

holds for $1 \leq i, j, k \leq s$. Upon applying χ_k to C_j we also note that

$$\chi_k(\mathsf{C}_j) = |\mathcal{C}_j| \chi_k(\mathcal{C}_j) \tag{3.5}$$

since the class function χ_k assumes the constant value $\chi_k(\mathcal{C}_j)$ on $\mathcal{C}_j$.

Since each C_j belongs to the center $Z(\mathbb{C}[\mathbf{G}])$ of $\mathbb{C}[\mathbf{G}]$ (in fact $\{\mathsf{C}_1, \mathsf{C}_2, \ldots, \mathsf{C}_s\}$ is a basis for $Z(\mathbb{C}[\mathbf{G}])$ by [2, Thm. 27.24] or [8, Thm. 2.4]) and each π_k is irreducible, it follows that $\pi_k(\mathsf{C}_j)$ is scalar for $1 \leq j, k \leq s$ (this follows from a standard version of Schur's Lemma [2, Thm. 29.13]). Thus there exist constants w_{jk} such that

$$\pi_k(\mathsf{C}_j) = w_{j,k} I_{d_k} \tag{3.6}$$

for $1 \leq j, k \leq s$ where $d_k = \dim \pi_k$ and I_{d_k} denotes the $d_k \times d_k$ identity matrix. Taking the trace of the preceding yields

$$\chi_k(\mathsf{C}_j) = d_k w_{j,k}. \tag{3.7}$$

Comparing (3.5) and (3.7) we find that

$$|\mathcal{C}_j| \chi_k(\mathcal{C}_j) = d_k w_{j,k},$$

which gives us the formula (3.1). Applying π_r to (4.1) and using (3.6) we obtain

$$w_{i,r} I_{d_r} w_{j,r} I_{d_r} = \sum_{k=1}^{s} c_{i,j,k} w_{kr} I_{d_r},$$

which clearly implies that

$$w_{i,r} w_{j,r} = \sum_{k=1}^{s} c_{i,j,k} w_{k,r}.$$

Now simply observe that the preceding is the (j,r)th entry of the matrix equation (3.2). Next we note that $W = \sqrt{|\mathbf{G}|}QUR$ where $R = \operatorname{diag}(d_1^{-1}, d_2^{-1}, \ldots, d_s^{-1})$. In particular, it follows that

$$\begin{aligned} QUD_iR &= QURD_i && (R, D_i \text{ are diagonal}) \\ &= M_iQUR && (\text{by (3.2)}) \end{aligned}$$

whence $QUD_i = M_iQU$ since R is invertible. Since Q is invertible this yields $T_iU = UD_i$ where $T_i = Q^{-1}M_iQ$. The fact that $|\mathbf{G}|^{-1/2}U$ is unitary (whence W is invertible) follows from the orthogonality of the irreducible characters $\chi_1, \chi_2, \ldots, \chi_s$. □

3.2. **Main construction.** We now apply Lemma 3.1 to the group $\mathbf{G}$ constructed in Section 2. As we shall see in Section 5, the matrices produced encode many of the basic properties of Kloosterman sums.

Recall that the (j,k) entry $(M_i)_{j,k}$ of M_i is defined to be the integer $c_{i,j,k}$ described in Lemma 3.1. Since $\mathbf{G}$ has four distinct types of conjugacy classes (see Table 2.1), we partition each M_i into 16 submatrices. As in Table 2.2 we adopt the convention that $f = p - 1$. It turns out that for $1 \le i \le f$ each of the M_i has basically the same structure as M_1, so we only display M_1 explicitly:

$$M_1 = \left(\begin{array}{cccc|cc|c|cccc} c_{1,1,1} & c_{1,1,2} & \cdots & c_{1,1,f} & 0 & 0 & f & 0 & 0 & \cdots & 0 \\ c_{1,2,1} & c_{1,2,2} & \cdots & c_{1,2,f} & 1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{1,f,1} & c_{1,f,2} & \cdots & c_{1,f,f} & 1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ \hline 0 & 1 & \cdots & 1 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 1 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \hline 1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & \cdots & 0 & 0 & 0 & 0 & f & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & f & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & f \end{array}\right). \tag{3.8}$$

We are interested primarily in studying the entries $c_{i,j,k}$ for $1 \le i, j, k \le f$ and we discuss them at length in Section 4.

In general, M_i for $2 \le i \le f$ differs from M_1 only in the upper-left 3×3 blocks. For instance the upper-left corner of M_2 looks like

$$\left(\begin{array}{ccccc|ccc} c_{2,1,1} & c_{2,1,2} & c_{2,1,3} & \cdots & c_{2,1,f} & 1 & 1 & 0 \\ c_{2,2,1} & c_{2,2,2} & c_{2,2,3} & \cdots & c_{2,2,f} & 0 & 0 & f \\ c_{2,3,1} & c_{2,3,2} & c_{2,3,3} & \cdots & c_{2,3,f} & 1 & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ c_{2,f,1} & c_{2,f,2} & c_{2,f,3} & \cdots & c_{2,f,f} & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & \cdots & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & \cdots & 1 & 1 & 0 & 0 \\ \hline 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \end{array}\right). \tag{3.9}$$

We therefore restrict our attention mostly to the case $i = 1$ since the computations for $i = 2, 3, \ldots, f$ are almost identical.

Examining the character table (Table 2.2) of $\mathbf{G}$ tells us that

$$D_i = \operatorname{diag}(K_{1i}, K_{2i}, \ldots, K_{(p-1)i}, -1, -1, \underbrace{f, f, \ldots, f}_{p-1 \text{ times}}), \tag{3.10}$$

$$Q = \operatorname{diag}(\underbrace{\sqrt{f}, \sqrt{f}, \ldots, \sqrt{f}}_{p+1 \text{ times}}, 1, \underbrace{p, p, \ldots, p}_{p-2 \text{ times}}),$$

and

$$W = \left(\begin{array}{cccc|cc|c|ccccc} K_1 & K_2 & \cdots & K_f & -1 & -1 & f & f & f & \cdots & f \\ K_2 & K_4 & \cdots & K_{2f} & -1 & -1 & f & f & f & \cdots & f \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ K_f & K_{2f} & \cdots & K_{f^2} & -1 & -1 & f & f & f & \cdots & f \\ \hline -1 & -1 & \cdots & -1 & f & -1 & f & f & f & \cdots & f \\ -1 & -1 & \cdots & -1 & -1 & f & f & f & f & \cdots & f \\ \hline 1 & 1 & \cdots & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ \hline 0 & 0 & \cdots & 0 & 0 & 0 & p^2 & p^2\xi & p^2\xi^2 & \cdots & p^2\xi^{p-2} \\ 0 & 0 & \cdots & 0 & 0 & 0 & p^2 & p^2\xi^2 & p^2\xi^4 & \cdots & p^2\xi^{2(p-2)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & p^2 & p^2\xi^{p-2} & p^2\xi^{2(p-2)} & \cdots & p^2\xi^{(p-2)^2} \end{array}\right).$$

Since Lemma 3.1 guarantees that the matrices $T_i := Q^{-1} M_i Q$ are simultaneously unitarily similar to the corresponding D_i's, each of which has only real entries, it follows from the Spectral Theorem that each T_i is hermitian. For instance,

$$T_1 = \left(\begin{array}{cccc|cc|c|ccccc} c_{1,1,1} & c_{1,1,2} & \cdots & c_{1,1,f} & 0 & 0 & \sqrt{f} & 0 & 0 & \cdots & 0 \\ c_{1,2,1} & c_{1,2,2} & \cdots & c_{1,2,f} & 1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{1,f,1} & c_{1,f,2} & \cdots & c_{1,f,f} & 1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ \hline 0 & 1 & \cdots & 1 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 1 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \hline \sqrt{f} & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & \cdots & 0 & 0 & 0 & 0 & f & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & f & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & f \end{array}\right).$$

Moreover, the unitary matrix U of Lemma 3.1 is given by

$$U = \frac{1}{p}\left(\begin{array}{cccc|cc|c|ccc|c} K_1 & K_2 & \cdots & K_f & -1 & -1 & 1 & 1 & 1 & \cdots & 1 \\ K_2 & K_4 & \cdots & K_{2f} & -1 & -1 & 1 & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ K_f & K_{2f} & \cdots & K_{f^2} & -1 & -1 & 1 & 1 & 1 & \cdots & 1 \\ \hline -1 & -1 & \cdots & -1 & f & -1 & 1 & 1 & 1 & \cdots & 1 \\ -1 & -1 & \cdots & -1 & -1 & f & 1 & 1 & 1 & \cdots & 1 \\ \hline \sqrt{f} & \sqrt{f} & \cdots & \sqrt{f} & \sqrt{f} & \sqrt{f} & \frac{1}{\sqrt{f}} & \frac{1}{\sqrt{f}} & \frac{1}{\sqrt{f}} & \cdots & \frac{1}{\sqrt{f}} \\ \hline 0 & 0 & \cdots & 0 & 0 & 0 & \frac{p}{\sqrt{f}} & \frac{p\xi}{\sqrt{f}} & \frac{p\xi^2}{\sqrt{f}} & \cdots & \frac{p\xi^{p-2}}{\sqrt{f}} \\ 0 & 0 & \cdots & 0 & 0 & 0 & \frac{p}{\sqrt{f}} & \frac{p\xi^2}{\sqrt{f}} & \frac{p\xi^4}{\sqrt{f}} & \cdots & \frac{p\xi^{2(p-2)}}{\sqrt{f}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \frac{p}{\sqrt{f}} & \frac{p\xi^{p-2}}{\sqrt{f}} & \frac{p\xi^{2(p-2)}}{\sqrt{f}} & \cdots & \frac{p\xi^{(p-2)^2}}{\sqrt{f}} \end{array}\right)$$

and it has the property that $T_iU = UD_i$. In particular, the kth column of U is an eigenvector of T_i corresponding to the kth diagonal entry of D_i.

In light of the block upper-triangular structure of U and the block of zeros in the upper-right of T_i, it follows that the equation $T_iU = UD_i$ still holds if we truncate all matrices involved to their upper left $(p+2)\times(p+2)$ blocks. We do so in order to remove entries that are irrelevant for our purposes and contain no useful information about Kloosterman sums. Performing this truncation we now consider instead the $(p+2)\times(p+2)$ matrices

$$\boxed{D_i = \operatorname{diag}(K_{1i}, K_{2i}, \ldots, K_{(p-1)i}, -1, -1, p-1)} \tag{3.11}$$

and

$$\boxed{T_i = \left(\begin{array}{cccc|cc|c} c_{i,1,1} & c_{i,1,2} & \cdots & c_{i,1,f} & 0 & 0 & \sqrt{f} \\ c_{i,2,1} & c_{i,2,2} & \cdots & c_{i,2,f} & 1 & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ c_{i,f,1} & c_{i,f,2} & \cdots & c_{i,f,f} & 1 & 1 & 0 \\ \hline 0 & 1 & \cdots & 1 & 0 & 1 & 0 \\ 0 & 1 & \cdots & 1 & 1 & 0 & 0 \\ \hline \sqrt{f} & 0 & \cdots & 0 & 0 & 0 & 0 \end{array}\right)\cdot} \tag{3.12}$$

Unfortunately, the new U obtained by truncating the original U is no longer unitary. However, this can easily be remedied by normalizing the $(p+2)$nd column, leading us to redefine U as follows:

$$\boxed{U = \frac{1}{p}\left(\begin{array}{cccc|cc|c} K_1 & K_2 & \cdots & K_f & -1 & -1 & \sqrt{f} \\ K_2 & K_4 & \cdots & K_{2f} & -1 & -1 & \sqrt{f} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ K_f & K_{2f} & \cdots & K_{f^2} & -1 & -1 & \sqrt{f} \\ \hline -1 & -1 & \cdots & -1 & f & -1 & \sqrt{f} \\ -1 & -1 & \cdots & -1 & -1 & f & \sqrt{f} \\ \hline \sqrt{f} & \sqrt{f} & \cdots & \sqrt{f} & \sqrt{f} & \sqrt{f} & 1 \end{array}\right)\cdot} \tag{3.13}$$

In summary, the truncated matrices (3.11), (3.12), and (3.13) satisfy $T_iU = UD_i$ for $1 \le i \le p-1$.

4. Submatrices of the T_i

For $i = 1, 2, \ldots, p-1$ we let $B_i = (c_{i,j,k})_{j,k=1}^{p-1}$ denote the upper left $(p-1)\times(p-1)$ submatrix of T_i (3.12). In this section we examine the structure of these matrices. Some of these properties will be used in Section 5 to study Kloosterman sums and in Section 6 to construct Ramanujan multigraphs.

4.1. **Computing the entries.** We claim that the entries of the B_i are given by

$$\boxed{c_{i,j,k} = 1 + \left(\frac{\beta(i,j,k)}{p}\right)} \tag{4.1}$$

where

$$\boxed{\beta(i,j,k) = i^2 + j^2 + k^2 - 2ij - 2jk - 2ik} \tag{4.2}$$

and $(\frac{\cdot}{p})$ denotes the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p. \end{cases}$$

In particular, it follows that $c_{i,j,k} \in \{0, 1, 2\}$ for all $1 \le i, j, k \le p-1$. In light of (4.1) and (4.2), we also have

$$c_{i,j,k} = c_{\sigma(i),\sigma(j),\sigma(k)} \tag{4.3}$$

for any permutation σ of $\{i, j, k\}$ and

$$c_{i,j,k} = c_{li,lj,lk} \tag{4.4}$$

for $1 \le i, j, k, l \le p-1$ (here the subscripts li, lj, lk are considered modulo p). Let us now justify the formula (4.1) for the entries of B_i.

According to Lemma 3.1, the entries $c_{i,j,k}$ denote the number of solutions $(X, Y) \in \mathcal{C}_i \times \mathcal{C}_j$ to the equation $XY = Z$ for some fixed $Z \in \mathcal{C}_k$. For $1 \le i, j, k \le p-1$ we consider the equation

$$\underbrace{\left(\begin{array}{cc|cc} 1 & ix & & \\ 0 & 1 & & \\ \hline & & 1 & x^{-1} \\ & & 0 & 1 \end{array}\right)}_{X\in\mathcal{C}_i} \underbrace{\left(\begin{array}{cc|cc} 1 & jy & & \\ 0 & 1 & & \\ \hline & & 1 & y^{-1} \\ & & 0 & 1 \end{array}\right)}_{Y\in\mathcal{C}_j} = \underbrace{\left(\begin{array}{cc|cc} 1 & k & & \\ 0 & 1 & & \\ \hline & & 1 & 1 \\ & & 0 & 1 \end{array}\right)}_{Z\in\mathcal{C}_k}, \tag{4.5}$$

which instantly reveals that $x^{-1} + y^{-1} = 1$ and $ix + jy = k$. Note that the first equation ensures that $x, y \neq 1$ so that $y = x(x-1)^{-1}$. Substituting this into the second equation we obtain the quadratic

$$ix^2 + (j - k - i)x + k = 0, \tag{4.6}$$

which has either 0, 1, or 2 solutions in $\mathbb{Z}/p\mathbb{Z}$. Since $k \neq 0$, it also follows that every solution x to (4.6) belongs to $(\mathbb{Z}/p\mathbb{Z})^\times$ and hence there is a bijective correspondence between solutions $(X, Y) \in \mathcal{C}_i \times \mathcal{C}_j$ to (4.5) and solutions $x \in \mathbb{Z}/p\mathbb{Z}$ to (4.6). Substituting $(2i)^{-1}[x - (j - k - i)]$ for x reveals that (4.6) has the same number of solutions as

$$x^2 = (j - k - i)^2 - 4ik = \beta(i, j, k)$$

where the function $\beta(i, j, k)$ is defined by (4.2). This establishes (4.1).

Before proceeding, we should remark that the appearance of the preceding quadratic is not surprising when one considers the well-known formula

$$K(u) = \sum_{n=0}^{p-1} \left(\frac{n^2 - 4u}{p} \right) \zeta^n, \tag{4.7}$$

which can be found in [4, Lem. 1.1], [15, eq. (1.6)], or [21, eq. (51)].

4.2. **Rows and columns.** Fix $1 \leq i, k \leq p-1$ and note that as X runs over the $p-1$ elements of $\mathcal{C}_i$, the variable $Y = X^{-1}Z$ runs over f distinct elements of $\mathbf{G}$. Therefore the sum of the kth column of M_i must equal f. In light of (3.8), we obtain the following formula for the column sums of the B_i:

$$\boxed{\sum_{j=1}^{p-1} c_{i,j,k} = \begin{cases} p-2 & \text{if } k = i, \\ p-3 & \text{if } k \neq i. \end{cases}} \tag{4.8}$$

By symmetry, the same formula holds for the row sums of B_i.

For $1 \leq i, j \leq p-1$ fixed we have

$$\beta(i,j,k) = k^2 - 2(i+j)k + (i-j)^2, \tag{4.9}$$

which we now consider as a quadratic in the variable k. By (4.1) it follows that $c_{i,j,k} = 1$ if and only if $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a root of the preceding quadratic. Since i and j are fixed, this holds for at most two values of k. Therefore each row (or column) of B_i can contain at most two 1's. Let us be more specific.

- Since $p-2$ is odd, it follows from (4.8) that the ith row of B_i contains exactly one 1. The remaining $p-2$ entries of the ith row are 0's and 2's which add up to $p-3$ by (4.8). Thus exactly $\frac{p-3}{2}$ of these entries are 2's and $\frac{p-1}{2}$ of them are 0's.
- Since $p-3$ is even, it follows from (4.8) that for $j \neq i$ the jth row of B_i contains either zero or two 1's. If the jth row contains zero 1's, then $\frac{p-3}{2}$ of its entries must be 2's. If the jth row contains two 1's, then $\frac{p-5}{2}$ of its entries must be 2's.
- Now suppose that $j \neq i$. We claim that if ij is a quadratic residue modulo p, then the jth row of B_i contains exactly two 1's and zero 1's otherwise. The only way to obtain a 1 in the jth column of B_i is for (4.9) to be congruent to 0 modulo p for some $1 \leq k \leq p-1$. Using the substitution $k \mapsto i + j + k \pmod{p}$, we see that this occurs if and only if

$$k^2 \equiv 4ij \pmod{p} \tag{4.10}$$

  for some k in $\{0, 1, 2, \ldots, i+j-1, i+j+1, \ldots, p-1\}$. The forbidden value $i+j$ poses no problem since if $(i+j)^2 \equiv 4ij \pmod{p}$, then $p|(i-j)$ whence $j = i$, contradicting our hypothesis that $j \neq i$. Thus (4.10) has a solution $k \neq i+j$ if and only if ij is a quadratic residue modulo p.

Putting this all together, we obtain Table 4.1, which describes the number of elements of each type in a given row/column of B_i. Using this data and the fact that there are exactly $\frac{p-3}{2}$ nonzero quadratic residues of the form ij ($j \neq i$) and $\frac{p-1}{2}$ nonresidues we can compute the total number of $0, 1, 2$'s in the matrix B_i (see

Row #	#0's	#1's	#2's
$j = i$	$\frac{p-1}{2}$	1	$\frac{p-3}{2}$
$j \neq i, (\frac{ij}{p}) = 1$	$\frac{p-1}{2}$	2	$\frac{p-5}{2}$
$j \neq i, (\frac{ij}{p}) = -1$	$\frac{p+1}{2}$	0	$\frac{p-3}{2}$

TABLE 4.1. Number of elements of each type in a given row of B_i. By symmetry, the same data applies to the columns of B_i.

	#0's	#1's	#2's
Total	$\frac{1}{2}p(p-1)$	$p-2$	$\frac{1}{2}(p-2)(p-3)$

TABLE 4.2. Total number of elements of each type in the matrix B_i. For large p the entries are roughly evenly split between 0's and 2's (i.e., approximately $\frac{1}{2}p^2$. On the other hand, the total number of 1's in the matrix is only of order p.

Table 4.2). We can also use this information to compute the sum of the squares of the entries of B_i (i.e., the quantity $\operatorname{tr} B_i^* B_i = \operatorname{tr} B_i^2$):

$$\begin{aligned} \operatorname{tr} B_i^2 &= (p-2) + 2(p-2)(p-3) \\ &= 2p^2 - 9p + 10. \end{aligned} \tag{4.11}$$

4.3. **Magical properties.** Along the main diagonal of B_i we have $j = k$ so that $c_{i,j,j} = 1 + (\frac{i^2-4ij}{p})$. For $j = 1, 2, \ldots, p-1$, this yields the sequence

$$i^2 - 4i,\ i^2 - 8i,\ \ldots,\ i^2 - 4i(p-1) \pmod p. \tag{4.12}$$

Note that the sequence $i^2 - 4ij = i(i-4j)$ cannot assume the value i^2 since $p \nmid 4j$. On the other hand, $i(i-4j)$ assumes every other value in $\mathbb{Z}/p\mathbb{Z}$ exactly once. Thus we conclude that 0 appears in the sequence (4.12) exactly once. Therefore exactly one of the diagonal entries of B_i is equal to 1. Since B_i is symmetric, it follows that there are an odd number of 1's among its entries, in agreement with the data in Table 4.2.

The trace of B_i is easily computed using the above. Since (4.12) assumes every value in $(\mathbb{Z}/p\mathbb{Z})^\times$ apart from 1, it follows that there are precisely $\frac{p-3}{2}$ nonzero quadratic residues on the list. Since we already know that a single 1 appears on the diagonal of B_i it follows that

$$\operatorname{tr} B_i = p - 2. \tag{4.13}$$

Next we observe that certain "broken diagonals" of B_i also enjoy curious summation properties. Indeed, using (4.3) and (4.4) for j and k fixed we have

$$\sum_{l=1}^{p-1} c_{i,lj,lk} = \sum_{l=1}^{p-1} c_{il^{-1},j,k} = \sum_{r=1}^{p-1} c_{r,j,k} = \sum_{r=1}^{p-1} c_{k,j,r} = \begin{cases} p-2 & \text{if } j = k, \\ p-3 & \text{if } j \neq k, \end{cases} \tag{4.14}$$

by (4.8). Define an equivalence relation $\sim$ on pairs (j,k) with $1 \leq j, k \leq p-1$ by setting $(j_1, k_1) \sim (j_2, k_2)$ if and only if $j_1 = lj_2 \pmod p$ and $k_1 = lk_2 \pmod p$ for some $1 \leq l \leq f$. This partitions the indices (j,k) into $p-1$ equivalence classes

of $p-1$ elements each, the sum over each equivalence class being given by the preceding formula.

Putting this all together we obtain two different "magic matrices" that are naturally associated to B_i. First observe from (4.8), (4.13), and (4.14) that if we subtract 1 from $c_{i,i,i}$ we obtain a new matrix B_i' for which each row, column, diagonal, and "broken diagonal" sums to $p-3$. For instance, if $p=7$ and we subtract 1 from the $(1,1)$ entry of B_1 we obtain the 6×6 "magic" matrix

Note: These matrices are best viewed in color (each broken diagonal is represented using a different color).

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 2 \\ 2 & 0 & 0 & 2 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 0 & 2 & 0 \end{pmatrix},$$

each row, column, and broken diagonal of which sums to 4.

We can also augment the $(p-1)\times(p-1)$ matrix B_i with one additional row and column from the larger matrix T_i to obtain a $p\times p$ matrix A_i which also enjoys "magic square" properties (i.e., A_i is the upper-left $p\times p$ principal submatrix of T_i). In particular, each row and column of A_i sums to $p-2$ while each diagonal and "broken diagonal" sums to $p-3$. For $p=11$, we obtain the 11×11 "magical" submatrix A_1 of T_1

$$\left(\begin{array}{cccccccccc|c} 0 & 0 & 0 & 1 & 2 & 2 & 0 & 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 & 1 & 2 & 0 & 2 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 1 \\ 2 & 0 & 1 & 0 & 2 & 0 & 2 & 0 & 1 & 0 & 1 \\ 2 & 2 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 2 & 0 & 2 & 0 & 2 & 1 \\ 0 & 0 & 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 1 \\ 2 & 0 & 0 & 1 & 1 & 0 & 0 & 2 & 2 & 0 & 1 \\ 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{array}\right).$$

In particular, note that each row and column sums to 9 while each broken diagonal sums to 8.

4.4. **Qualitative behavior of eigenvalues.** By the triangle inequality one obtains the trivial bound $|K(a,b)|\le p-1$ for all a,b. However, a significant amount of cancellation can occur in the sum (1.1). The famous *Weil bound* asserts that

$$|K(a,b)|\le 2\sqrt{p}, \tag{4.15}$$

whenever $p\nmid ab$ [23]. A complete proof, based on Stepanov's method [22], can be found in the recent text [9, Thm. 11.11].

For a $n\times n$ real symmetric matrix X we let

$$\lambda_0(X)\le\lambda_1(X)\le\cdots\le\lambda_{n-1}(X)$$

denote the eigenvalues of X, repeated according to multiplicity. We are concerned here with the qualitative behavior of the eigenvalues of the $(p+2)\times(p+2)$ matrix $T:=T_1$ (3.12) and its $p\times p$ upper-left principal submatrix $A:=A_1$.

p	$-2\sqrt{p}$	$\lambda_0(T)$	$\lambda_0(A)$	$\lambda_{p-2}(A)$	$\lambda_{p+1}(T)$	$2\sqrt{p}$
7	−5.2915	−2.69202	−2.55594	**3.87311**	4.49396	5.2915
11	−6.63325	−5.71695	**−5.3493**	4.48588	4.79575	6.63325
29	−10.7703	−9.50028	**−9.43532**	8.89626	9.06824	10.7703
71	−16.8523	−15.8699	**−15.8149**	14.1059	14.1728	16.8523
113	−21.2603	−20.9713	**−20.8836**	19.5715	19.6731	21.2603
229	−30.2655	−29.8296	−29.75	**29.9351**	30.0001	30.2655
379	−38.9358	−38.2481	**−38.2008**	37.4232	37.4756	38.9358
541	−46.5188	−46.4712	**−46.4221**	46.3519	46.3885	46.5188
863	−58.7537	−58.5638	**−58.5258**	57.613	57.6483	58.7537
1223	−69.9428	−67.6103	−67.5843	**69.0147**	69.0451	69.9428
1583	−79.5739	−79.328	**−79.3055**	77.3993	77.4206	79.5739
1987	−89.1516	−88.7625	−88.7417	**88.7745**	88.7849	89.1516

TABLE 4.3. The smallest and the second largest eigenvalues of the $(p+2)\times(p+2)$ matrix T and its $(p-1)\times(p-1)$ principal submatrix A.

By the Weil bound (4.15) and a standard result relating the eigenvalues of a hermitian matrix to those of a principal submatrix [6, Thm. 4.3.15] we have

$$-2\sqrt{p} \le \lambda_j(T) \le \lambda_j(A) \le \lambda_{j+2}(T) \le 2\sqrt{p}$$

for $0 \le j \le p-2$. In particular, it follows from (4.15) and the preceding chain of inequalities that

$$-2\sqrt{p} \le \lambda_0(T) \le \lambda_0(A) \le \lambda_2(T) \tag{4.16}$$

and

$$\lambda_{p-1}(T) \le \lambda_{p-1}(A) \le \lambda_{p+1}(T) \le 2\sqrt{p}. \tag{4.17}$$

Using the Weil bound, we now write

$$K(u) = 2\sqrt{p}\cos\theta_p(u)$$

where $\theta_p(u) \in [0,\pi]$. The *vertical Sato-Tate law* [1, 11] states that as $p \to \infty$ the sequence of angles $\theta_p(u)$ becomes equidistributed with respect to the *Sato-Tate measure* $\mu = \frac{2}{\pi}\sin^2\theta\, d\theta$ on $[0,\pi]$. Thus for any fixed $\delta > 0$ there are at least three values of $\theta_p(u)$ in each of the intervals $[0,\delta]$ and $[\pi-\delta,\pi]$ when p is sufficiently large. In light of (4.16) and (4.17), we see that $\lim_{p\to\infty}\lambda_0(A) = -2\sqrt{p}$ and $\lim_{p\to\infty}\lambda_{p-2}(A) = 2\sqrt{p}$. This behavior is clearly reflected in Table 4.3, even for relatively small values of p.

The preceding argument relies upon a deep result of Katz [11]. On the other hand, the matrix A is quite concrete and it enjoys many unusual combinatorial properties (Subsection 4.3). One might hope to estimate the eigenvalues of A directly to obtain an elementary proof of a Weil-type bound. The following result indicates that the error incurred using such an approach would not change the order of magnitude of the resulting estimate.

Theorem 4.1. *If $p \ge 5$ is an odd prime, then*

$$\max\{|K(u)| : u = 0,1,\dots,p-1\} \le \max\{|\lambda_0(A)|, |\lambda_{p-2}(A)|\} + \sqrt{p-1}.$$

In other words, an estimate of the form $\max\{|\lambda_0(A)|, |\lambda_{p-2}(A)|\} \le C\sqrt{p}$ leads to a Weil-type estimate of the form $\max\{|K(u)|\} \le C'\sqrt{p}$.

Proof. First note that if A_{ij} are block matrices of the appropriate size, then

$$\left\| \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mn} \end{pmatrix} \right\| \leq \left\| \begin{pmatrix} \|A_{11}\| & \|A_{12}\| & \cdots & \|A_{1n}\| \\ \|A_{21}\| & \|A_{22}\| & \cdots & \|A_{2n}\| \\ \vdots & \vdots & \ddots & \vdots \\ \|A_{m1}\| & \|A_{m2}\| & \cdots & \|A_{mn}\| \end{pmatrix} \right\|.$$

Moreover, if each A_{ij} is a nonnegative multiple of an all 1's matrix, then equality holds. Therefore

$$\begin{aligned} \|T - A \oplus 0_{3\times 3}\| &= \left\| \left(\begin{array}{c|ccc|c|c} 0 & 0 & \cdots & 0 & 0 & \sqrt{p-1} \\ \hline 0 & 0 & \cdots & 0 & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ \hline 0 & 1 & \cdots & 1 & 0 & 0 \\ \hline \sqrt{p-1} & 0 & \cdots & 0 & 0 & 0 \end{array} \right) \right\| \\ &= \left\| \begin{pmatrix} 0 & 0 & 0 & \sqrt{p-1} \\ 0 & 0 & \sqrt{p-2} & 0 \\ 0 & \sqrt{p-2} & 0 & 0 \\ \sqrt{p-1} & 0 & 0 & 0 \end{pmatrix} \right\| \\ &= \sqrt{p-1}. \end{aligned}$$

The theorem now follows from the triangle inequality for the operator norm. □

5. Applications to Kloosterman sums

In the following, we employ the matrices $T = T_1$ (3.12), $D = D_1$ (3.11), and U (3.13) constructed in Subsection 3.2. As before, we let $A = A_1$ and $B = B_1$ denote the upper-left $p \times p$ and $(p-1) \times (p-1)$ principal submatrices of T.

5.1. **Basic Kloosterman identities.** Using the character table of $\mathbf{G}$ (Table 2.2) we can derive a number of identities involving Kloosterman sums. For instance, taking the inner product of the first column with the $(p+2)$th column yields

$$\boxed{\sum_{u=0}^{p-1} K(u) = 0.} \tag{5.1}$$

In particular, this gives another proof of (4.13) since $\operatorname{tr} B = \operatorname{tr} T = \operatorname{tr} D = f - 1 + \sum_{u=0}^{p-1} K(u) = p - 2$.

If $c \neq 0$, then taking the inner product of the first and the cth of the columns of the character table leads to

$$\boxed{\sum_{u=0}^{p-1} K(u)K(cu) = -p.} \tag{5.2}$$

Taking the inner product of the first column with itself we find that

$$\begin{aligned} \sum_{u=0}^{p-1} K^2(u) + p \cdot 1^2 &= \#C_{\mathbf{G}} \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right) \\ &= \# \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} : y, z \in \mathbb{Z}/p\mathbb{Z} \right\} \\ &= p^2, \end{aligned}$$

where $C_{\mathbf{G}}(\cdot)$ denotes the centralizer of an element of $\mathbf{G}$. This yields the well-known formula [15, eq. 3.7]:

$$\boxed{\sum_{u=0}^{p-1} K^2(u) = p^2 - p.} \tag{5.3}$$

Since the matrices D and T (given by (3.11) and (3.12), respectively) are unitarily similar, it follows that the sums of the squares of their entries must be equal (i.e., $\operatorname{tr} D^2 = \operatorname{tr} T^2$). Thus

$$\underbrace{(p^2-p) + (-1)^2 + (p-1)^2}_{\operatorname{tr} D^2} = \underbrace{\operatorname{tr} B^2 + 2(p-1) + 4(p-2) + 2}_{\operatorname{tr} T^2} \tag{5.4}$$

by (5.3). The preceding also yields $\operatorname{tr} B^2 = 2p^2 - 9p + 10$, which provides another proof of (4.11). In fact, since we already have an independent proof of (4.11), we could work backward from (5.4) to provide another proof of (5.3).

From (5.2) and (5.3) we obtain (for $c \neq 0, 1$)

$$\sum_{u=0}^{p-1} [K(u) - K(cu)]^2 = 2p^2, \tag{5.5}$$

$$\sum_{u=0}^{p-1} [K(u) + K(cu)]^2 = 2p^2 - 4p. \tag{5.6}$$

Other such quadratic identities (e.g., [15, eqs. 3.5, 3.8]) might be deduced from Table 2.2 using the generalized orthogonality relations [8, Thm. 2.13]:

$$\frac{1}{|\mathbf{G}|} \sum_{G \in \mathbf{G}} \chi_i(GH)\chi_j(G^{-1}) = \delta_{i,j} \frac{\chi_i(H)}{\chi_i(I)}.$$

Applying [10, Thm. 30.4] (see also [8, Prob. 3.9]) we obtain the formula

$$c_{i,j,k} = \frac{|\mathbf{G}|}{|C_{\mathbf{G}}(G_i)||C_{\mathbf{G}}(G_j)|} \sum_{u=1}^{2p} \frac{\chi_u(G_i)\chi_u(G_j)\overline{\chi_u(G_k)}}{\chi_u(I)},$$

which for $i = 1$ and $1 \leq j, k \leq p-1$ yields an identity equivalent to [13, Prop. 6.2]:

$$\sum_{u=0}^{p-1} K(u)K(ju)K(ku) = \left(\frac{\beta(1,j,k)}{p}\right) p^2 + 2p$$

(this can also be easily deduced by computing the (j,k) entry of $T = UDU$). By (4.2) we have $\beta(1,1,1) = -3$ from which we obtain [14, eq. 1], [15, eq. 3.22], and [21, eq. (70)]:

$$\boxed{\sum_{u=0}^{p-1} K^3(u) = \begin{cases} p^2 + 2p & \text{if } p \equiv 1 \pmod 3, \\ -p^2 + 2p & \text{if } p \equiv 2 \pmod 3. \end{cases}} \tag{5.7}$$

5.2. **Quartic formulas and Kloosterman's bound.** Computing the (j,j) entry of $T^2 = UD^2U$, we obtain

$$\underbrace{\frac{1}{p^2}\left(\sum_{u=0}^{p-1} K(u)^2K(ju)^2 + 1 + f^3\right)}_{(j,j)\text{ entry of } UD^2U} = \underbrace{\begin{cases} 1+2(p-3)+f & \text{if } j=1, \\ 2+2(p-5)+2 & \text{if } j\neq 1 \text{ and } (\frac{j}{p})=1, \\ 2(p-3)+2 & \text{if } j\neq 1 \text{ and } (\frac{j}{p})=-1, \end{cases}}_{(j,j)\text{ entry of } T^2 \text{ obtained from Table 4.1}}$$

leading us to [13, Prop. 6.3] and [15, eq. 3.18]:

$$\boxed{\sum_{u=0}^{p-1} K^2(u)K^2(ju) = \begin{cases} 2p^3-3p^2-3p & \text{if } j=1, \\ p^3-3p^2-3p & \text{if } j\neq 1 \text{ and } (\frac{j}{p})=1, \\ p^3-p^2-3p & \text{if } j\neq 1 \text{ and } (\frac{j}{p})=-1. \end{cases}} \tag{5.8}$$

Based upon this we obtain the following result of Kloosterman himself [12].

Theorem 5.1 (Kloosterman)**.** *$|K(u)| < 2^{\frac{1}{4}}p^{\frac{3}{4}}$ for all u.*

Proof. Let $j=1$ in (5.8), observe that $|K(u)|^4 < 2p^3$, then take fourth roots. □

We remark that the simple proof above achieves a better constant (namely $2^{\frac{1}{4}}$ in place of $3^{\frac{1}{4}}$ – see also [21, eq. 72]) than the recent proof in [5].

Although it is not clear whether one can obtain the Weil bound (4.15) using these methods, we have at least demonstrated that the unitary similarity $A = UDU^*$ encodes enough information about Kloosterman sums to obtain nontrivial results. Furthermore, we can establish that the exponent $\frac{1}{2}$ appearing in the Weil bound cannot be improved. Indeed, from (5.3) and (5.8) we have

$$\begin{aligned} 2p^3-3p^2-3p = \sum_{u=0}^{p-1} K(u)^4 &\leq \max\{K(u)^2\}\sum_{u=0}^{p-1} K^2(u) \\ &\leq \max\{K(u)^2\}(p^2-p) \end{aligned}$$

whence

$$\max\{K(u)^2\} \geq \frac{2p^2-3p-3}{p-1} = 2p-2+\frac{p-5}{p-1} > 2(p-1).$$

In other words, there exists some u such that

$$|K(u)| \geq \sqrt{2}(p-1)^{\frac{1}{2}}. \tag{5.9}$$

5.3. **Symmetric functions of Kloosterman sums.** Recall that the coefficients c_j in the expansion

$$\det(X-\lambda I) = c_0\lambda^n + c_1\lambda^{n-1} + \cdots + c_n$$

of the characteristic polynomial of a $n\times n$ matrix X are given by Bôcher's recursion

$$c_0 = 1, \qquad c_j = -\frac{1}{j}\left[c_{j-1}\operatorname{tr}X + c_{j-2}\operatorname{tr}X^2 + \cdots + c_0\operatorname{tr}X^j\right].$$

Applying this procedure to the diagonal matrix $X = \operatorname{diag}(K_0, K_1, \ldots, K_{p-1})$ and using (5.1), (5.3), (5.7), and (5.8), we obtain $c_0 = 1$, $c_1 = 0$,

$$\begin{aligned} c_2 &= \tfrac{1}{2}(\operatorname{tr}^2 X - \operatorname{tr}X^2) \\ &= -\tfrac{1}{2}(p^2-p), \end{aligned}$$

$$\begin{aligned} c_3 &= -\tfrac{1}{6}\left[(\operatorname{tr} X)^3 + 2\operatorname{tr} X^3 - 3(\operatorname{tr} X)(\operatorname{tr} X^2)\right] \\ &= -\frac{p}{3}\left[\left(\frac{-3}{p}\right)p + 2\right], \\ c_4 &= \tfrac{1}{24}\left[(\operatorname{tr} X)^4 - 6(\operatorname{tr} X)^2(\operatorname{tr} X^2) + 3(\operatorname{tr} X^2)^2 + 8(\operatorname{tr} X)(\operatorname{tr} X^3) - 6\operatorname{tr} X^4\right] \\ &= \tfrac{1}{8}p(p-3)(p^2-3p-2). \end{aligned}$$

We therefore obtain

$$\boxed{\prod_{u=0}^{p-1}(\lambda - K_u) = \lambda^p - \frac{1}{2}(p^2-p)\lambda^{n-2} - \frac{p}{3}\left[\left(\frac{-3}{p}\right)p + 2\right]\lambda^{n-3} + \cdots,} \tag{5.10}$$

which agrees with [15, p. 403]. The preceding now yields formulas for certain symmetric functions of Kloosterman sums:

$$\begin{aligned} \sum_{0\le j<k\le p-1} K_jK_k &= -\frac{1}{2}(p^2-p), \\ \sum_{0\le i<j<k\le p-1} K_iK_jK_k &= \frac{p}{3}\left[\left(\frac{-3}{p}\right)p + 2\right], \\ \sum_{0\le i<j<k<l\le p-1} K_iK_jK_kK_l &= \tfrac{1}{8}p(p-3)(p^2-3p-2). \end{aligned}$$

A different approach to (5.10) can be based upon the fact that the matrix

$$X = \left(\begin{array}{cccc|cc|c} c_{1,1,1} & c_{1,1,2} & \cdots & c_{1,1,f} & 0 & 0 & f \\ c_{1,2,1} & c_{1,2,2} & \cdots & c_{1,2,f} & 1 & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ c_{1,f,1} & c_{1,f,2} & \cdots & c_{1,f,f} & 1 & 1 & 0 \\ \hline 0 & 1 & \cdots & 1 & 0 & 1 & 0 \\ 0 & 1 & \cdots & 1 & 1 & 0 & 0 \\ \hline 1 & 0 & \cdots & 0 & 0 & 0 & 0 \end{array}\right)$$

is similar to the diagonal matrix $D = \operatorname{diag}(K_1, K_2, \ldots, K_f, -1, -1, f)$ (3.11). Indeed, the first matrix is similar to the truncated matrix T (3.12), which is itself unitarily similar to D. Using the fact that one may add a multiple of one row (resp. column) to another inside a determinant, one easily obtains [13, Lem. 14]:

Theorem 5.2. *The Kloosterman sums $K_0, K_1, K_2, \ldots, K_f$ are precisely the eigenvalues of the matrix*

$$\left(\begin{array}{cccc|c} c_{1,1,1}-f & c_{1,1,2}-f & \cdots & c_{1,1,f}-f & -f \\ c_{1,2,1} & c_{1,2,2} & \cdots & c_{1,2,f} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{1,f,1} & c_{1,f,2} & \cdots & c_{1,f,f} & 1 \\ \hline 0 & 2 & \cdots & 2 & 1 \end{array}\right),$$

where the coefficients $c_{i,j,k}$ are defined by (4.1) *and $f = p-1$.*

Before proceeding, we remark that modifications of our main construction apply to various generalizations of classical Kloosterman sums. For instance, one might consider the Galois field $\mathbb{F}_{p^n}$ in place of $\mathbb{Z}/p\mathbb{Z}$. Moreover, our general scheme also

applies to hyper-Kloosterman sums (the appropriate analogue of our group $\mathbf{G}$ is discussed in [13, p. 16]).

6. Ramanujan multigraphs

Certain principal submatrices of the T_i can be used to construct multigraphs having desirable spectral properties. To be more specific, a *multigraph* is a graph that is permitted to have multiple edges and loops.[1]

Associated to a multigraph $\mathcal{G}$ is its adjacency matrix $A(\mathcal{G})$, the real symmetric matrix whose rows and columns are indexed by the vertices $v_1, v_2, \ldots, v_n$ of $\mathcal{G}$ and whose (j,k) entry $a_{j,k}$ is the number of edges connecting v_k to v_j. In particular, if $j = k$ then $a_{j,j}$ counts the number of loops attached to the vertex v_j. We refer to the eigenvalues of $A(\mathcal{G})$ as the *eigenvalues of* $\mathcal{G}$.

The *degree* of a vertex is the number of edges terminating at that vertex. We say that a multigraph $\mathcal{G}$ is *d-regular* if each vertex has degree d. In this case d is an eigenvalue of $\mathcal{G}$ with corresponding eigenvector $(1, 1, \ldots, 1)$. On the other hand, $-d$ is an eigenvalue of $\mathcal{G}$ if and only if $\mathcal{G}$ is bipartite, in which case the multiplicity of $-d$ corresponding to the number of connected components of $\mathcal{G}$. An easy application of the Gerschgorin disk theorem indicates that every eigenvalue of $\mathcal{G}$ belongs to the interval $[-d, d]$. We therefore label the eigenvalues of a d-regular multigraph $\mathcal{G}$, according to their multiplicity, as follows:

$$d \geq \lambda_0(\mathcal{G}) \geq \lambda_1(\mathcal{G}) \geq \cdots \geq \lambda_{n-1}(\mathcal{G}) \geq -d.$$

The eigenvalues of $\mathcal{G}$ of a d-regular multigraph which lie in the open interval $(-d, d)$ are called the *nontrivial eigenvalues* of $\mathcal{G}$. We let $\lambda(\mathcal{G})$ denote the absolute value of the nontrivial eigenvalue of $\mathcal{G}$ which is largest in magnitude.

Following [20], we say that a *Ramanujan multigraph* is a d-regular multigraph $\mathcal{G}$ satisfying

$$\lambda(\mathcal{G}) \leq 2\sqrt{d-1}.$$

For instance, the Petersen graph is an example of a 3-regular Ramanujan graph (see Figure 1). There is a vast literature dedicated to the study of *simple* (i.e., no

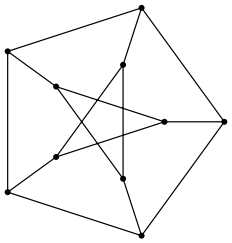

FIGURE 1. The Petersen graph is 3-regular and has characteristic polynomial $(z-3)(z+2)^4(z-1)^5$. The nontrivial eigenvalues 1 and -2 are both smaller than $2\sqrt{2}$ in absolute value whence the Petersen graph is Ramanujan.

loops or multiple edges) Ramanujan graphs. We refer the reader to the seminal papers [16, 18, 19] and the texts [3] and [17] for more information.

[1]The terminology in the literature is somewhat inconsistent. The term *multigraph* is sometimes reserved for graphs with multiple edges but no loops. If loops are present, then the term *pseudograph* is used.

We are now in a position to construct a family of Ramanujan multigraphs:

Theorem 6.1. *Let $p \geq 5$ be an odd prime, $1 \leq i \leq p-1$, and let $\beta(i,j,k)$ be given by* (4.2).

(1) *The multigraph $\mathcal{G}$ whose adjacency matrix is given by the matrix*

$$a_{j,k} = 1 + \left(\frac{\beta(i,j,k)}{p}\right)$$

is a $(p-2)$-regular Ramanujan multigraph on p vertices.

(2) *If $p \equiv 3 \pmod 4$, then setting $a_{i,i} = 1$ and*

$$a_{j,k} = 1 + \left(\frac{\beta(i,j,k)}{p}\right)$$

otherwise yields a $(p-3)$-regular Ramanujan multigraph on $p-1$ vertices.

Proof. The regularity of the resulting multigraphs are ensured by (4.8) and the general form (3.12) of T_i. The fact that they are Ramanujan follows from (4.16) and (4.17). □

For instance, letting $p = 7$ and $i = 1$ we obtain the adjacency matrix

$$A = \begin{pmatrix} 2 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 2 & 1 \\ 2 & 0 & 0 & 2 & 0 & 0 & 1 \\ 1 & 1 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 2 & 1 \\ 0 & 2 & 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \tag{6.1}$$

corresponding to the multigraph depicted in Figure 2.

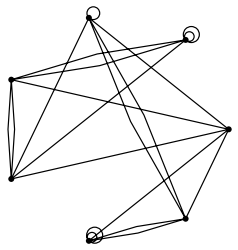

FIGURE 2. The Ramanujan multigraph corresponding to the adjacency matrix (6.1).

REFERENCES

[1] Alan Adolphson. On the distribution of angles of Kloosterman sums. *J. Reine Angew. Math.*, 395:214–220, 1989.

[2] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[3] Giuliana Davidoff, Peter Sarnak, and Alain Valette. *Elementary number theory, group theory, and Ramanujan graphs*, volume 55 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2003.

[4] Benji Fisher. Distinctness of Kloosterman sums. In *p-adic methods in number theory and algebraic geometry*, volume 133 of *Contemp. Math.*, pages 81–102. Amer. Math. Soc., Providence, RI, 1992.
[5] D. R. Heath-Brown. Arithmetic applications of Kloosterman sums. *Nieuw Arch. Wiskd. (5)*, 1(4):380–384, 2000.
[6] Roger A. Horn and Charles R. Johnson. *Matrix analysis*. Cambridge University Press, Cambridge, 1990. Corrected reprint of the 1985 original.
[7] Norman E. Hurt. Kloosterman sums and their applications: a review. *Results Math.*, 29(1-2):16–41, 1996.
[8] 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].
[9] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.
[10] Gordon James and Martin Liebeck. *Representations and characters of groups*. Cambridge University Press, New York, second edition, 2001.
[11] Nicholas M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.
[12] 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.
[13] Philip C. Kutzko. The cyclotomy of finite commutative P.I.R.'s. *Illinois J. Math.*, 19:1–17, 1975.
[14] D. H. Lehmer and Emma Lehmer. On the cubes of Kloosterman sums. *Acta Arith.*, 6:15–22, 1960.
[15] D. H. Lehmer and Emma Lehmer. The cyclotomy of Kloosterman sums. *Acta Arith.*, 12:385–407, 1966/67.
[16] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.
[17] Alexander Lubotzky. *Discrete groups, expanding graphs and invariant measures*, volume 125 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 1994. With an appendix by Jonathan D. Rogawski.
[18] G. A. Margulis. Explicit constructions of expanders. *Problemy Peredači Informacii*, 9(4):71–80, 1973.
[19] Moshe Morgenstern. Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q. *J. Combin. Theory Ser. B*, 62(1):44–62, 1994.
[20] M. Ram Murty. Ramanujan graphs. *J. Ramanujan Math. Soc.*, 18(1):33–52, 2003.
[21] Hans Salié. Über die Kloostermanschen Summen $S(u, v; q)$. *Math. Z.*, 34(1):91–109, 1932.
[22] S. A. Stepanov. The number of points of a hyperelliptic curve over a finite prime field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 33:1171–1181, 1969.
[23] André Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U. S. A.*, 34:204–207, 1948.

Mathematics and Computer Science Department, South Dakota School of Mines and Technology, 501 East Saint Joseph Street, Rapid City, South Dakota 57701
E-mail address: Patrick.Fleming@sdsmt.edu

Department of Mathematics, Pomona College, 610 N. College Ave, Claremont, California, 91711
E-mail address: Stephan.Garcia@pomona.edu
URL: http://pages.pomona.edu/~sg064747

E-mail address: Gizem.Karaali@pomona.edu
URL: http://pages.pomona.edu/~gk014747