Ramanujan J
DOI 10.1007/s11139-013-9478-y

Ramanujan sums as supercharacters

Christopher F. Fowler · Stephan Ramon Garcia · Gizem Karaali

Received: 23 December 2012 / Accepted: 9 March 2013

Abstract The theory of *supercharacters*, recently developed by Diaconis-Isaacs and André, is used to derive the fundamental algebraic properties of Ramanujan sums. This machinery frequently yields one-line proofs of difficult identities and provides many novel formulas. In addition to exhibiting a new application of supercharacter theory, this article also serves as a blueprint for future work since some of the abstract results we develop are applicable in much greater generality.

Keywords Ramanujan sum · Multiplicative function · Arithmetic function · Even function modulo n · Supercharacter theory · Representation · Supercharacter · Kronecker product

Mathematics Subject Classification Primary 11L03, 11A25 · Secondary 20C15

1 Introduction

Our primary aim in this note is to demonstrate that most of the fundamental algebraic properties of Ramanujan sums can be deduced using the theory of *supercharacters*,

S.R. Garcia partially funded by NSF grant DMS-1001614. G. Karaali partially funded by a NSA Young Investigator Award.

C.F. Fowler
Department of Mathematics, University of Washington, Box 354350, Seattle, WA 98195-4350, USA
e-mail: cff2008@math.washington.edu

S.R. Garcia (✉) · G. Karaali
Department of Mathematics, Pomona College, Claremont, CA 91711, USA
e-mail: Stephan.Garcia@pomona.edu
url: http://pages.pomona.edu/~sg064747

G. Karaali
e-mail: Gizem.Karaali@pomona.edu
url: http://pages.pomona.edu/~gk014747

Published online: 17 July 2013

recently developed by Diaconis-Isaacs and André. In fact, the machinery of supercharacter theory frequently yields one-line proofs of many difficult identities and provides an array of new tools that can be used to derive various novel formulas. Our approach is entirely systematic, relying on a flexible and general framework. Indeed, we hope to convince the reader that supercharacter theory provides a natural framework for the study of Ramanujan sums. In addition to exhibiting a novel application of supercharacter theory, this article also serves as a blueprint for future work since some of the abstract results we develop are applicable in much greater generality (see [10] for recent developments).

1.1 Ramanujan sums

In what follows, we let $e(x) = \exp(2\pi i x)$, so that the function $e(x)$ is periodic with period 1. For integers n, x with $n \geq 1$, the expression

$$c_n(x) = \sum_{\substack{j=1 \\ (j,n)=1}}^{n} e\left(\frac{jx}{n}\right) \tag{1.1}$$

is called a *Ramanujan sum* (or sometimes *Ramanujan's sum*). Ramanujan himself (1918) [53, Paper 21] noted that Dirichlet and Dedekind had already considered such expressions in their famed text *Vorlesungen über Zahlentheorie* (1863). Moreover, certain related identities were already known to von Sterneck (1902) [63], Kluyver (1906) [36], Landau (1909) [39], and Jensen (1915) [28]. Nevertheless, "Ramanujan was the first to appreciate the importance of the sum and to use it systematically," according to G.H. Hardy [19, p. 159].

Ramanujan's interest in the sums (1.1) originated in his desire to "obtain expressions for a variety of well-known arithmetical functions of n in the form of a series $\sum_s a_s c_s(n)$." This particular analytic aspect of the subject has flourished in the intervening years and is discussed at length in [41, 43, 56, 57]. On the other hand, in classical character theory Ramanujan sums can be used to establish the integrality of the character values for the symmetric group [27, Cor. 22.17]. However, perhaps the most famous appearance of Ramanujan sums is their crucial role in Vinogradov's proof that every sufficiently large odd number is the sum of three primes [46, Chap. 8].

In more recent years, Ramanujan sums have appeared in the study of Waring-type formulas [37], the distribution of rational numbers in short intervals [33], equirepartition modulo odd integers [8], the large sieve inequality [54], graph theory [16], symmetry classes of tensors [59], combinatorics [55], cyclotomic polynomials [17, 44, 47, 62], and Mahler matrices [40]. In physics, Ramanujan sums have applications in the processing of low-frequency noise [49] and of long-period sequences [48] and in the study of quantum phase locking [50]. We should also remark that various generalizations of the classical Ramanujan sum (1.1) have arisen over the years [2, 11, 12, 58] and that Ramanujan sums involving matrix variables have also been considered [45, 52].

1.2 Supercharacters

The theory of supercharacters, of which classical character theory is a special case, was recently introduced by Diaconis and Isaacs (2008) [14] to generalize the *basic characters* of André [3–5]. Here we summarize a few important facts. Further details can be found in [14, 23].

Definition (Diaconis–Isaacs [14]) Let G be a finite group, let $\mathcal{K}$ be a partition of G, and let $\mathcal{X}$ be a partition of the set $\mathrm{Irr}(G)$ of irreducible characters of G. We call the ordered pair $(\mathcal{X}, \mathcal{K})$ a *supercharacter theory* if

(1) $\{1\} \in \mathcal{K}$;
(2) $|\mathcal{X}| = |\mathcal{K}|$;
(3) for each $X \in \mathcal{X}$, the character

$$\sigma_X = \sum_{\chi \in X} \chi(1)\chi$$

is constant on each $K \in \mathcal{K}$.

The characters σ_X are called *supercharacters*, and the elements K of $\mathcal{K}$ are called *superclasses*.

As [14, Lemma 2.1] shows, the preceding definition is equivalent to the following.

Definition (André [6]) Let G be a finite group, let $\mathcal{K}$ be a partition of G, and let $\mathcal{X}$ be a collection of complex characters of G. We call the ordered pair $(\mathcal{X}, \mathcal{K})$ a *supercharacter theory* if

(1) every irreducible character of G is a constituent of a unique $\chi \in \mathcal{X}$;
(2) $|\mathcal{X}| = |\mathcal{K}|$;
(3) each character $\chi \in \mathcal{X}$ is constant on K for each $K \in \mathcal{K}$.

The elements χ of $\mathcal{X}$ are called *supercharacters*, and the sets K are called *superclasses*.

Regardless of which definition one chooses to work with, it is straightforward to verify that each K in $\mathcal{K}$ is a union of conjugacy classes of G and that each of the partitions $\mathcal{K}$ and $\mathcal{X}$ determines the other. The only significant difference between these two definitions is that the second approach can yield supercharacters that are multiples of the σ_X defined above.

In the literature to date, the main use of supercharacter theory has been to perform computations when a complete character theory is difficult or impossible to determine. For instance, André developed a successful supercharacter theory for the unipotent matrix groups $U_n(q)$ whose representation theories are known to be *wild* (see also [64, 65]). Supercharacter theories have also proven to be relevant outside the realm of finite group theory. For instance, these notions can be used to obtain a more general theory of spherical functions and Gelfand pairs [14]. In a different direction, recent work has revealed deep connections between supercharacter theory and the Hopf algebra of symmetric functions of noncommuting variables [1]. Another application may be found in [7], where the authors use supercharacter theory to study random walks on upper triangular matrices. Other recent work on supercharacters concerns connections with Schur rings [23, 25] and with their combinatorial properties [15, 60, 61]. We should also remark that similar constructions surfaced independently in the study of quasigroups and association schemes in the form of *fusions* of character tables [25, 29, 32].

1.3 General approach

We proceed along a different course, turning our attention to the group $\mathbb{Z}/n\mathbb{Z}$, whose classical representation theory is already well understood. It turns out that a natural supercharacter theory for $\mathbb{Z}/n\mathbb{Z}$ can be developed for which Ramanujan sums appear as values of the corresponding supercharacters. In this manner, the modern machinery of supercharacter theory can be used to generate a wide variety of formulas and identities for Ramanujan sums. Along the way, we also develop a notion of *superclass arithmetic*, which generalizes the standard arithmetic of conjugacy classes from classical character theory.

2 A supercharacter theory for $\mathbb{Z}/n\mathbb{Z}$

In this section we introduce a supercharacter theory for $\mathbb{Z}/n\mathbb{Z}$, which arises naturally from the action of $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ on $\mathbb{Z}/n\mathbb{Z}$ (see [9] for a description of all possible supercharacter theories on $\mathbb{Z}/n\mathbb{Z}$). Before proceeding, we require a few preliminaries. Although some of this material is well known in certain circles, we include the details since the theory of supercharacters is not yet common knowledge among the general mathematics community. Moreover, for many of the upcoming applications, we require a particular unitary rescaling of our supercharacter tables which is not widely used.

2.1 Supercharacter tables

Suppose that G is a finite group of order $|G|$ and that $(\mathcal{X},\mathcal{K})$ is a supercharacter theory for G. In other words, suppose that we have a partition $\mathcal{X}=\{X_1,X_2,\ldots,X_r\}$ of $\mathrm{Irr}(G)$ with corresponding supercharacters

$$\sigma_i=\sum_{\chi\in X_i}\chi(1)\chi \tag{2.1}$$

and a compatible partition $\mathcal{K}=\{K_1,K_2,\ldots,K_r\}$ of G into superclasses. The *supercharacter table* for G corresponding to $(\mathcal{X},\mathcal{K})$ is the $r\times r$ array

$$\begin{array}{c|cccc} & K_1 & K_2 & \cdots & K_r \\ \hline \sigma_1 & \sigma_1(K_1) & \sigma_1(K_2) & \cdots & \sigma_1(K_r) \\ \sigma_2 & \sigma_2(K_1) & \sigma_2(K_2) & \cdots & \sigma_2(K_r) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_r & \sigma_r(K_1) & \sigma_r(K_2) & \cdots & \sigma_r(K_r) \end{array}, \tag{2.2}$$

whose (i, j) entry is $\sigma_i(K_j)$. We let

$$S = \big(\sigma_i(K_j)\big)_{i,j=1}^{r}$$

denote the $r \times r$ matrix that encodes the data in (2.2). In what follows we frequently identify supercharacter tables with their matrix representations, and we often refer to the matrix S itself as a supercharacter table.

Recall that a function $f : G \to \mathbb{C}$ is called a *class function* if f is constant on each conjugacy class of G. The space of complex-valued class functions on G is endowed with the natural inner product

$$\langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi'(g)}, \tag{2.3}$$

with respect to which the irreducible characters of G form an orthonormal basis. In light of the fact that supercharacters are constant on superclasses (i.e., they are *superclass functions*), (2.3) implies that

$$\langle \sigma_i, \sigma_j \rangle = \frac{1}{|G|} \sum_{\ell=1}^{r} |K_\ell| \sigma_i(K_\ell)\overline{\sigma_j(K_\ell)}.$$

It follows from (2.1) and the orthogonality of irreducible characters that

$$\langle \sigma_i, \sigma_j \rangle = \left\langle \sum_{\chi \in X_i} \chi(1)\chi, \sum_{\chi' \in X_j} \chi'(1)\chi' \right\rangle = \delta_{i,j} \|X_i\|_2^2,$$

where

$$\|X_i\|_2 = \sqrt{\sum_{\chi \in X_i} |\chi(1)|^2}$$

is a convenient shorthand. Putting this all together, we see that

$$\frac{1}{|G|} \sum_{\ell=1}^{r} |K_\ell| \sigma_i(K_\ell)\overline{\sigma_j(K_\ell)} = \delta_{i,j} \|X_i\|_2^2. \tag{2.4}$$

It is helpful to interpret the preceding result matricially. Letting

$$R = \operatorname{diag}\big(\sqrt{|K_1|}, \sqrt{|K_2|}, \ldots, \sqrt{|K_r|}\big), \tag{2.5}$$

we see that (2.4) is equivalent to asserting that

$$(SR)(SR)^* = |G| \operatorname{diag}\big(\|X_1\|_2^2, \|X_2\|_2^2, \ldots, \|X_r\|_2^2\big).$$

Letting

$$L = \frac{1}{\sqrt{|G|}} \operatorname{diag}\big(\|X_1\|_2^{-1}, \|X_2\|_2^{-1}, \ldots, \|X_r\|_2^{-1}\big), \tag{2.6}$$

we conclude that the matrix

$$U = LSR \tag{2.7}$$

satisfies $UU^* = I$. In other words, the $r \times r$ matrix

$$U = \frac{1}{\sqrt{|G|}}\left[\frac{\sigma_i(K_j)\sqrt{|K_j|}}{\|X_i\|_2}\right]_{i,j=1}^{r} \tag{2.8}$$

is unitary. Since $U^*U = I$, we now obtain the column orthogonality relation

$$\frac{\sqrt{|K_i||K_j|}}{|G|}\sum_{\ell=1}^{r}\frac{\sigma_\ell(K_i)\overline{\sigma_\ell(K_j)}}{\|X_\ell\|_2^2} = \delta_{i,j}. \tag{2.9}$$

Similarly, we see that the equation $UU^* = I$ encodes (2.4).

2.2 A supercharacter table for $\mathbb{Z}/n\mathbb{Z}$

As remarked in [14], each subgroup H of $\mathrm{Aut}(G)$ determines a corresponding supercharacter theory $(\mathcal{X}_H, \mathcal{K}_H)$ for G. To be more specific, H induces a permutation of $\mathrm{Irr}(G)$ while also permuting the conjugacy classes of G. By Brauer's lemma [26, Thm. 6.32, Cor. 6.33], the number of H-orbits of $\mathrm{Irr}(G)$ equals the number of H-orbits induced on the set of conjugacy classes of G. This decomposition yields a supercharacter theory for G where the elements X_i of $\mathcal{X}_H = \{X_1, X_2, \ldots, X_r\}$ are H-orbits in $\mathrm{Irr}(G)$ and the superclasses K_i of $\mathcal{K}_H = \{K_1, K_2, \ldots, K_r\}$ are unions of H-orbits of conjugacy classes of G. By construction, each supercharacter (2.1) is constant on each member of $\mathcal{K}_H$.

Fix a positive integer n and let $\tau(n)$ denote the number of divisors of n. Let $d_1, d_2, \ldots, d_{\tau(n)}$ denote the divisors of n, the exact order being unimportant for our purposes at the moment. Recall that the irreducible characters of $\mathbb{Z}/n\mathbb{Z}$ are precisely the functions

$$\chi_a(x) = e\left(\frac{ax}{n}\right)$$

for $a = 1, 2, \ldots, n$ and that each automorphism of $\mathbb{Z}/n\mathbb{Z}$ is of the form

$$\psi_u(a) = ua$$

for some u in $(\mathbb{Z}/n\mathbb{Z})^\times$. In particular, we note that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Next we observe that there exists a u in $(\mathbb{Z}/n\mathbb{Z})^\times$ such that $\psi_u(a) = b$ if and only if $(a, n) = (b, n)$. In light of the fact that $\chi_a \circ \psi_u = \chi_{au}$, it is clear that the action of $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ on $\mathrm{Irr}(\mathbb{Z}/n\mathbb{Z})$ partitions the irreducible characters into a disjoint collection $\mathcal{X} = \{X_1, X_2, \ldots, X_{\tau(n)}\}$ of orbits

$$X_i = \left\{\chi_a : (a, n) = \frac{n}{d_i}\right\},$$

each of which satisfies

$$|X_i| = \phi(d_i), \tag{2.10}$$

where ϕ denotes the Euler totient function. Thus,

$$\sigma_i(x) = \sum_{\chi \in X_i} \chi(x) = \sum_{\substack{j=1 \\ (j,n)=\frac{n}{d_i}}}^{n} e\left(\frac{jx}{n}\right) = \sum_{\substack{k=1 \\ (k,d_i)=1}}^{d_i} e\left(\frac{kx}{d_i}\right) = c_{d_i}(x), \tag{2.11}$$

each of which is a Ramanujan sum. On the other hand, the action of $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ on $\mathbb{Z}/n\mathbb{Z}$ results in a partition $\mathcal{K} = \{K_1, K_2, \ldots, K_{\tau(n)}\}$ of $\mathbb{Z}/n\mathbb{Z}$ into disjoint orbits

$$K_j = \left\{a \in \mathbb{Z}/n\mathbb{Z} : (a,n) = \frac{n}{d_j}\right\}, \tag{2.12}$$

each of which satisfies

$$|K_j| = \phi(d_j). \tag{2.13}$$

Since each conjugacy class of $\mathbb{Z}/n\mathbb{Z}$ is a singleton, it is clear that the proposed superclass (2.12) is the union of conjugacy classes.

Let us pause briefly to note that since $c_n(x)$ is a superclass function with respect to the variable x, we obtain the following useful fact:

$$c_n\big((x,n)\big) = c_n(x). \tag{2.14}$$

In other words, $c_n(x)$ is an *even function modulo n* [43, p. 79], [57, p. 15].

Putting this all together, we obtain the $\tau(n) \times \tau(n)$ supercharacter table $S(n)$

	K_1	K_2	$\cdots$	$K_{\tau(n)}$
σ_1	$c_{d_1}(\frac{n}{d_1})$	$c_{d_1}(\frac{n}{d_2})$	$\cdots$	$c_{d_1}(\frac{n}{d_{\tau(n)}})$
σ_2	$c_{d_2}(\frac{n}{d_1})$	$c_{d_2}(\frac{n}{d_2})$	$\cdots$	$c_{d_2}(\frac{n}{d_{\tau(n)}})$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\sigma_{\tau(n)}$	$c_{d_{\tau(n)}}(\frac{n}{d_1})$	$c_{d_{\tau(n)}}(\frac{n}{d_2})$	$\cdots$	$c_{d_{\tau(n)}}(\frac{n}{d_{\tau(n)}})$

,

whose (i,j) entry is given by

$$\big[S(n)\big]_{i,j} = c_{d_i}\left(\frac{n}{d_j}\right). \tag{2.15}$$

When there is no chance of confusion, we simply write $S = S(n)$. We leave the particular order in which the divisors $d_1, d_2, \ldots, d_{\tau(n)}$ of n are listed unspecified, noting only that any pair of orderings lead to two matrices that are similar via a suitable permutation matrix. Such relationships between matrices will arise frequently in what follows, and we therefore introduce the following notation. We shall write $A \cong B$ whenever A and B are square matrices such that $B = P^{-1}AP$ for some permutation matrix P. Although we use the same symbol to denote the isomorphism of groups, the meaning should be clear from context.

Before moving on, let us recall that pre- and post-multiplying S by the diagonal matrices L, given by (2.6), and R, given by (2.5), yield the unitary matrix $U = LSR$. In light of (2.10) and (2.13), it turns out that $L = (\sqrt{n}R)^{-1}$, whence

$$\sqrt{n}U = R^{-1}SR. \tag{2.16}$$

In other words, the supercharacter table $S(n)$ is similar to a multiple of the unitary matrix $U = U(n)$ given by

$$\frac{1}{\sqrt{n}}\begin{bmatrix} c_{d_1}(\frac{n}{d_1}) & c_{d_1}(\frac{n}{d_2})\sqrt{\frac{\phi(d_2)}{\phi(d_1)}} & \cdots & c_{d_1}(\frac{n}{d_{\tau(n)}})\sqrt{\frac{\phi(d_{\tau(n)})}{\phi(d_1)}} \\ c_{d_2}(\frac{n}{d_1})\sqrt{\frac{\phi(d_1)}{\phi(d_2)}} & c_{d_2}(\frac{n}{d_2}) & \cdots & c_{d_2}(\frac{n}{d_{\tau(n)}})\sqrt{\frac{\phi(d_{\tau(n)})}{\phi(d_2)}} \\ \vdots & \vdots & \ddots & \vdots \\ c_{d_{\tau(n)}}(\frac{n}{d_1})\sqrt{\frac{\phi(d_1)}{\phi(d_{\tau(n)})}} & c_{d_{\tau(n)}}(\frac{n}{d_2})\sqrt{\frac{\phi(d_2)}{\phi(d_{\tau(n)})}} & \cdots & c_{d_{\tau(n)}}(\frac{n}{d_{\tau(n)}}) \end{bmatrix}. \tag{2.17}$$

Example 1 If p is a prime number, then the two divisors $d_1 = 1$ and $d_2 = p$ of p lead to the corresponding superclasses $K_1 = \{p\}$ and $K_2 = \{1, 2, \dots, p-1\}$ of $\mathbb{Z}/p\mathbb{Z}$. A short computation now reveals that

$$S(p) = \begin{bmatrix} 1 & 1 \\ p-1 & -1 \end{bmatrix}, \qquad U(p) = \frac{1}{\sqrt{p}}\begin{bmatrix} 1 & \sqrt{p-1} \\ \sqrt{p-1} & -1 \end{bmatrix}. \tag{2.18}$$

In particular, observe that $U(p)$ is a selfadjoint unitary involution which has only real entries. It turns out, as we shall see, that this is true for general $U(n)$.

2.3 Orthogonality relations

Using the row and column orthogonality relations (2.4) and (2.9), we immediately obtain

$$\sum_{k|n}\phi(k)c_{d_i}\left(\frac{n}{k}\right)c_{d_j}\left(\frac{n}{k}\right) = \begin{cases} 0 & \text{if } i \neq j, \\ n\phi(d_i) & \text{if } i = j, \end{cases} \tag{2.19}$$

and

$$\sum_{k|n}\frac{1}{\phi(k)}c_k\left(\frac{n}{d_i}\right)c_k\left(\frac{n}{d_j}\right) = \begin{cases} 0 & \text{if } i \neq j, \\ \frac{n}{\phi(d_i)} & \text{if } i = j, \end{cases} \tag{2.20}$$

respectively. The first is a well-known identity [57, Thm. 3.1.e, p. 16], and the second is somewhat lesser known [43, Ex. 2.22]. If $d|n$, then letting $d_i = d$ and $d_j = 1$ in (2.19), we obtain [43, Ex. 2.24]

$$\sum_{k|n}\phi(k)c_d\left(\frac{n}{k}\right) = \begin{cases} 0 & \text{if } d \neq 1, \\ n & \text{if } d = 1. \end{cases}$$

3 Multiplicativity and Kronecker products

In this section, we consider product supercharacter theories and their ramifications for the study of Ramanujan sums. In particular, it turns out that many of the peculiar multiplicative properties of Ramanujan sums can be easily derived by examining Kronecker products of supercharacter tables. In addition to providing simple proofs of many standard identities, our techniques will ultimately permit the derivation of many novel identities as well (e.g., the bizarre determinantal formula (3.23) and the power sum identities of Sect. 4.5).

3.1 Prime powers

In the following, we let p denote a fixed prime number. For each $\alpha \geq 1$, let us identify the supercharacter table $S = S(p^\alpha)$ that arises from the action of $\mathrm{Aut}(\mathbb{Z}/p^\alpha\mathbb{Z}) \cong (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ on the group $\mathbb{Z}/p^\alpha\mathbb{Z}$. Before proceeding, it is helpful to note that

$$c_{p^m}(x) = \begin{cases} p^{m-1}(p-1) & \text{if } p^m | x, \\ -p^{m-1} & \text{if } p^m \nmid x \text{ but } p^{m-1} | x, \\ 0 & \text{otherwise}, \end{cases} \tag{3.1}$$

which can be computed easily from the definition (1.1) and the formula for the sum of a finite geometric series. Among other things, we note that

$$c_{p^m}(1) = \mu\big(p^m\big), \qquad c_{p^m}\big(p^m\big) = \phi\big(p^m\big), \tag{3.2}$$

where $\mu(n)$ denotes the *Möbius μ-function*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is not square-free}, \\ (-1)^\omega & \text{if } n \text{ is the product of } \omega \text{ distinct primes}. \end{cases} \tag{3.3}$$

Since the divisors of p^α are precisely the numbers $d_i = p^{i-1}$ for $i = 1, 2, \ldots, \alpha+1$, (2.15) and (3.1) tell us that the (i, j) entry of the $(\alpha+1) \times (\alpha+1)$ matrix $S = S(p^\alpha)$ is given by

$$\big[S\big(p^\alpha\big)\big]_{i,j} = c_{p^{i-1}}\big(p^{\alpha-j+1}\big) = \begin{cases} 1 & \text{if } i = 1, \\ p^{i-2}(p-1) & \text{if } i + j \leq \alpha + 2, \\ -p^{i-2} & \text{if } i + j = \alpha + 3, \\ 0 & \text{if } i + j > \alpha + 3. \end{cases} \tag{3.4}$$

For instance, the supercharacter tables $S(p^2)$ and $S(p^3)$ are given by

$$\left[\begin{array}{c|cc} 1 & 1 & 1 \\ p-1 & p-1 & -1 \\ \hline p(p-1) & -p & 0 \end{array}\right], \qquad \left[\begin{array}{c|ccc} 1 & 1 & 1 & 1 \\ p-1 & p-1 & p-1 & -1 \\ p(p-1) & p(p-1) & -p & 0 \\ \hline p^2(p-1) & -p^2 & 0 & 0 \end{array}\right], \tag{3.5}$$

respectively. In general, $S(p^{\alpha-1})$ appears as the upper-right hand corner of $S(p^\alpha)$, as illustrated in (3.5). Let us also note, for future reference, that

$$\operatorname{tr} S(p^\alpha) = \begin{cases} p^{\frac{\alpha}{2}} & \text{if } \alpha \text{ is even,} \\ 0 & \text{if } \alpha \text{ is odd,} \end{cases} \tag{3.6}$$

follows from (3.4) and a telescoping series argument.

For some purposes, it is more fruitful to consider the associated unitary matrix $U = U(p^\alpha)$, defined by (2.17), in place of $S(p^\alpha)$ itself. Setting $n = p^\alpha$, $d_i = p^{i-1}$, and $d_j = p^{j-1}$ in (2.17), we find that

$$[U(p^\alpha)]_{i,j} = \frac{c_{p^{i-1}}(p^{\alpha-j+1})\sqrt{\phi(p^{j-1})}}{p^{\alpha/2}\sqrt{\phi(p^{i-1})}}. \tag{3.7}$$

A few simple computations reveal that

$$[U(p^\alpha)]_{i,j} = \begin{cases} p^{-\frac{\alpha}{2}} & \text{if } i=j=1, \\ p^{\frac{j-\alpha-2}{2}}\sqrt{p-1} & \text{if } i=1 \text{ and } j>1, \\ p^{\frac{i-\alpha-2}{2}}\sqrt{p-1} & \text{if } j=1 \text{ and } i>1, \\ (p-1)p^{\frac{i+j-\alpha-4}{2}} & \text{if } 3 \le i+j \le \alpha+2, \\ -\frac{1}{\sqrt{p}} & \text{if } 3 \le i+j = \alpha+3, \\ 0 & \text{if } i+j > \alpha+3. \end{cases} \tag{3.8}$$

Despite its somewhat imposing appearance, the preceding expression tells us that the $(\alpha+1)\times(\alpha+1)$ unitary matrix U is selfadjoint and that its lower right $\alpha\times\alpha$ submatrix is a Hankel matrix. This is illustrated in the following example.

Example 2

$$U(2^6) = \left[\begin{array}{c|cccccc} \frac{1}{8} & \frac{1}{8} & \frac{1}{4\sqrt{2}} & \frac{1}{4} & \frac{1}{2\sqrt{2}} & \frac{1}{2} & \frac{1}{\sqrt{2}} \\ \hline \frac{1}{8} & \frac{1}{8} & \frac{1}{4\sqrt{2}} & \frac{1}{4} & \frac{1}{2\sqrt{2}} & \frac{1}{2} & -\frac{1}{\sqrt{2}} \\ \frac{1}{4\sqrt{2}} & \frac{1}{4\sqrt{2}} & \frac{1}{4} & \frac{1}{2\sqrt{2}} & \frac{1}{2} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{2\sqrt{2}} & \frac{1}{2} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2} & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

Since $U = U(n)$ is unitary and selfadjoint, it follows that

$$U^2 = I. \tag{3.9}$$

Therefore the only possible eigenvalues of U are ± 1. The exact multiplicities of these eigenvalues can be determined using (2.16), which asserts that $p^{\alpha/2}U$ is similar to S. It follows from (3.6) that

$$\operatorname{tr} U = \begin{cases} 1 & \text{if } \alpha \text{ is even,} \\ 0 & \text{if } \alpha \text{ is odd.} \end{cases} \tag{3.10}$$

Since U is $(\alpha+1)\times(\alpha+1)$, it follows that the eigenvalues of U are -1 (multiplicity $\frac{\alpha}{2}$) and 1 (multiplicity $\frac{\alpha}{2}+1$) if α is even; and ± 1 (both with multiplicity $\frac{\alpha+1}{2}$) if α is odd. Since

$$\left\lfloor \frac{\alpha+1}{2} \right\rfloor = \begin{cases} \frac{\alpha}{2} & \text{if } \alpha \text{ is even,} \\ \frac{\alpha+1}{2} & \text{if } \alpha \text{ is odd,} \end{cases}$$

we conclude that

$$\det U\bigl(p^{\alpha}\bigr) = (-1)^{\lfloor \frac{\alpha+1}{2} \rfloor}. \tag{3.11}$$

We will make use of this formula later on.

3.2 Kronecker products

Recall that the *Kronecker product* $A \otimes B$ of an $m \times n$ matrix A and a $p \times q$ matrix B is the $mp \times nq$ matrix given by

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}.$$

Whenever the dimensions of the matrices involved are compatible, we have $A \otimes B \cong B \otimes A$ and

$$(A \otimes B)(C \otimes D) \cong AC \otimes BD,$$

where, as briefly mentioned in Sect. 2.2, $\cong$ denotes similarity via a permutation matrix. Finally, we also recall that if A is $m \times m$ and B is $n \times n$, then

$$\det(A \otimes B) = (\det A)^n (\det B)^m \tag{3.12}$$

and

$$\operatorname{tr}(A \otimes B) = (\operatorname{tr} A)(\operatorname{tr} B). \tag{3.13}$$

3.3 Products of supercharacter theories

Given two supercharacter theories $(\mathcal{X}_1, \mathcal{K}_1)$ and $(\mathcal{X}_2, \mathcal{K}_2)$ on two finite groups G_1 and G_2, one can construct a natural product supercharacter theory on $G_1 \times G_2$. Writing

$$\mathcal{K}_1 = \bigl\{K_1^{(1)}, K_2^{(1)}, \ldots, K_r^{(1)}\bigr\}, \qquad \mathcal{K}_2 = \bigl\{K_1^{(2)}, K_2^{(2)}, \ldots, K_s^{(2)}\bigr\},$$

and

$$\mathcal{X}_1 = \{X_1^{(1)}, X_2^{(1)}, \ldots, X_r^{(1)}\}, \qquad \mathcal{X}_2 = \{X_1^{(2)}, X_2^{(2)}, \ldots, X_s^{(2)}\},$$

we first define

$$\mathcal{K} = \mathcal{K}_1 \times \mathcal{K}_2. \tag{3.14}$$

On the other hand, since [26, Thm. 4.21] tells us that

$$\operatorname{Irr}(G_1 \times G_2) = \operatorname{Irr}(G_1) \times \operatorname{Irr}(G_2),$$

it is natural for us to define

$$\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2. \tag{3.15}$$

A straightforward computation now shows that

$$\sigma_{X_i^{(1)} \times X_j^{(2)}}\big((g_1, g_2)\big) = \sigma_{X_i^{(1)}}(g_1)\sigma_{X_j^{(2)}}(g_2) \tag{3.16}$$

whenever g_1 and g_2 belong to G_1 and G_2, respectively. In particular, this implies that $\sigma_{X_1 \times X_2}$ is constant on each element of $\mathcal{K}$. Since $|\mathcal{X}| = |\mathcal{X}_1||\mathcal{X}_2| = |\mathcal{K}_1||\mathcal{K}_2| = |\mathcal{K}|$, we conclude that $(\mathcal{X}, \mathcal{K})$ is a supercharacter theory on $G_1 \times G_2$.

Putting this all together, (3.16) tells us that if S_1 and S_2 are the matrices that encode the supercharacter tables corresponding to the supercharacter theories $(\mathcal{X}_1, \mathcal{K}_1)$ and $(\mathcal{X}_2, \mathcal{K}_2)$ on G_1 and G_2, respectively, then the Kronecker product $S_1 \otimes S_2$ encodes the product supercharacter theory $(\mathcal{X}, \mathcal{K})$ on $G_1 \times G_2$. To be more specific, we list the elements of $\mathcal{K}$ and $\mathcal{X}$ in their respective lexicographic orders induced by the product structures (3.14) and (3.15). In light of (3.16), we see that the resulting supercharacter table S for the product theory $(\mathcal{X}, \mathcal{K})$ on $G_1 \times G_2$ satisfies $S \cong S_1 \otimes S_2$.

The details of the preceding construction were worked out by A.O.F. Hendrickson, a student of Isaacs, in his doctoral thesis [22, Sect. 2.6]. We refer the reader there and to his recent paper [23] for further information.

3.4 Multiplicativity

Recall that if G_1 and G_2 are finite groups, then

$$\operatorname{Aut}(G_1) \times \operatorname{Aut}(G_2) \subseteq \operatorname{Aut}(G_1 \times G_2),$$

although equality does not hold in general. We are interested here in the special case where $G_1 = \mathbb{Z}/m\mathbb{Z}$, $G_2 = \mathbb{Z}/n\mathbb{Z}$, and $(m, n) = 1$. In this setting,

$$(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/mn\mathbb{Z}, \tag{3.17}$$

so that if we indulge in a slight abuse of language, we obtain

$$\operatorname{Aut}(\mathbb{Z}/m\mathbb{Z}) \times \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \subseteq \operatorname{Aut}(\mathbb{Z}/mn\mathbb{Z})$$

or, equivalently,

$$(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \subseteq (\mathbb{Z}/mn\mathbb{Z})^\times.$$

Since the orders of the preceding groups are $\phi(m)$, $\phi(n)$, and $\phi(mn)$, respectively, it follows from the multiplicativity of the Euler totient function that

$$\operatorname{Aut}(\mathbb{Z}/m\mathbb{Z}) \times \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \operatorname{Aut}(\mathbb{Z}/mn\mathbb{Z}).$$

Thus the product supercharacter theory for $\mathbb{Z}/mn\mathbb{Z}$, obtained from the supercharacter theories for $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ induced by $\operatorname{Aut}(\mathbb{Z}/m\mathbb{Z})$ and $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$, respectively, is the same supercharacter theory for $\mathbb{Z}/mn\mathbb{Z}$ that arises from the action of $\operatorname{Aut}(\mathbb{Z}/mn\mathbb{Z})$. In other words,

$$S(mn) \cong S(m) \otimes S(n) \tag{3.18}$$

whenever $(m,n)=1$. In particular, it follows from (3.16) and the Chinese Remainder Theorem that

$$c_{mn}\big(dd'\big) = c_m(d)c_n\big(d'\big) \tag{3.19}$$

whenever d and d' are positive divisors of m and n, respectively. Indeed, first let $G_1 = \mathbb{Z}/m\mathbb{Z}$ and $G_2 = \mathbb{Z}/n\mathbb{Z}$, with

$$K^1_{\tau(m)} = \big\{a \in \mathbb{Z}/m\mathbb{Z} : (a,m)=1\big\}, \qquad K^2_{\tau(n)} = \big\{b \in \mathbb{Z}/n\mathbb{Z} : (a,n)=1\big\},$$

and observe that the map $\Phi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z}$ defined by $\Phi((a,b)) = ab \pmod{mn}$ is an isomorphism. In particular, this implies that

$$\Phi\big(K^1_{\tau(m)} \times K^2_{\tau(n)}\big) = \big\{c \in \mathbb{Z}/mn\mathbb{Z} : (c,mn)=1\big\}$$

and that

$$\Phi\big(\big(d,d'\big)\big) = dd' \pmod{mn}$$

whenever $d|m$ and $d'|n$. Putting this all together and using (3.16) leads to the desired formula (3.19).

Now recall that when we originally defined the supercharacter table $S(n)$ for $\mathbb{Z}/n\mathbb{Z}$ (see Sect. 2.2), we were not particular about the manner in which the divisors of n were listed. The reason for this lack of specificity is due to the fact that even though the Kronecker product $S(m) \otimes S(n)$ represents a supercharacter table for $\mathbb{Z}/mn\mathbb{Z}$ arising from the action of $\operatorname{Aut}(\mathbb{Z}/mn\mathbb{Z})$, the ordering of the superclasses and supercharacters in the product table might differ from what one might consider a "natural" ordering (e.g., the ordering induced by listing the divisors of mn in increasing or decreasing order). However, this poses no difficulty in practice since much of our work will involve similarity invariants of matrices.

Example 3 For $m=4$ and $n=5$ and using the ordered divisor lists $\{1,2,4\}$ and $\{1,5\}$, respectively, from (3.4) we obtain

$$S(4) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -2 & 0 \end{bmatrix}, \qquad S(5) = \begin{bmatrix} 1 & 1 \\ 4 & -1 \end{bmatrix}.$$

Using the ordered divisor list $\{1, 2, 4, 5, 10, 20\}$ for $mn = 20$ and computing $S(20)$ directly from (2.15) and the definition of Ramanujan sums yields

$$S(20) = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 \\ 2 & -2 & 0 & 2 & -2 & 0 \\ \hline 4 & 4 & 4 & -1 & -1 & -1 \\ 4 & 4 & -4 & -1 & -1 & 1 \\ 8 & -8 & 0 & -2 & 2 & 0 \end{array}\right] = S(5) \otimes S(4).$$

In the preceding we have partitioned the matrix $S(20)$ for clarity.

An important consequence of (3.19) is the fact that Ramanujan sums $c_n(x)$ are multiplicative with respect to the subscript n.

Theorem 3.1 *If* $(m, n) = 1$, *then*

$$c_{mn}(x) = c_m(x)c_n(x)$$

for all x *in* $\mathbb{Z}$.

Proof Since $(m, n) = 1$, it follows from (3.19) that

$$c_{mn}\big((x, mn)\big) = c_{mn}\big((x, m)(x, n)\big) = c_m\big((x, m)\big)c_n\big((x, n)\big),$$

whence $c_{mn}(x) = c_m(x)c_n(x)$ by (2.14). □

Corollary 3.2 *For* $n \geq 1$, *we have*

$$c_n(1) = \mu(n), \qquad c_n(n) = \phi(n).$$

Furthermore, $c_n(x)$ *is always an integer.*

Proof The boxed statements follow from (3.2) and Theorem 3.1. The integrality of $c_n(x)$ follows from Theorem 3.1 and the explicit values given in (3.4). □

The proof of Theorem 3.1 suggests an interesting variant [43, Ex. 2.2, p. 89]:

Theorem 3.3 *If* $(mx, ny) = 1$, *then*

$$c_{mn}(xy) = c_m(x)c_n(y). \tag{3.20}$$

Proof Since $(m, n) = (x, n) = (y, m) = 1$, it follows from (3.19) that

$$c_{mn}\big((xy, mn)\big) = c_{mn}\big((x, m)(y, n)\big) = c_m\big((x, m)\big)c_n\big((y, n)\big),$$

whence $c_{mn}(xy) = c_m(x)c_n(y)$ by (2.14). □

Corollary 3.4 *If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is the canonical factorization of n into distinct primes $p_1, p_2, \ldots, p_r$ and $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ is a divisor of n, then*

$$c_n(d) = \prod_{\ell=1}^{r} c_{p_\ell^{\alpha_\ell}}\big(p_\ell^{\beta_\ell}\big).$$

3.5 Piecing things together

The following useful result permits us to deduce a variety of results about Ramanujan sums by piecing together our observations from Sect. 3.1. In the present setting, recall that product supercharacter theories correspond to Kronecker products of supercharacter tables.

Theorem 3.5 *If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is the canonical factorization of n into distinct primes $p_1, p_2, \ldots, p_r$, then*

$$S(n) \cong \bigotimes_{i=1}^{r} S\big(p_i^{\alpha_i}\big), \qquad U(n) \cong \bigotimes_{i=1}^{r} U\big(p_i^{\alpha_i}\big). \tag{3.21}$$

In particular, $U(n)$ is a selfadjoint, unitary involution whose (i, j) entry is given by

$$\big[U(n)\big]_{i,j} = \frac{1}{\sqrt{n}} c_{d_i}\left(\frac{n}{d_j}\right)\sqrt{\frac{\phi(d_j)}{\phi(d_i)}}, \tag{3.22}$$

where $d_1, d_2, \ldots, d_{\tau(n)}$ are the positive divisors of n. We also have $S(n)^2 = nI$.

Proof The first matrix identity in (3.21) follows immediately from (3.18). The second identity in (3.21) follows from the first identity, the multiplicativity of (3.7), and the basic properties of the Kronecker product, along with (2.16), (2.5), and (2.13). The fact that $U(n)$ is a selfadjoint involution follows from the fact that each $U(p_i^{\alpha_i})$ is a selfadjoint involution. Formula (3.22) is a simple consequence of (3.7) and the multiplicativity of the Euler totient function. Finally, we note that (2.16) now implies that $S(n)^2 = nI$. □

As a trivial consequence of Theorem 3.5, we obtain [43, Ex. 2.10]:

Corollary 3.6 *For $n \geq 1$, we have*

$$\sum_{d|n} c_d\left(\frac{n}{d}\right) = \begin{cases} 0 & \text{if } n \text{ is not a perfect square,} \\ \sqrt{n} & \text{if } n \text{ is a perfect square.} \end{cases}$$

Proof Writing $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ and applying (3.21), we find that

$$\sum_{d|n} c_d\left(\frac{n}{d}\right) = \operatorname{tr} S(n) = \operatorname{tr}\left(\bigotimes_{i=1}^{r} S\big(p_i^{\alpha_i}\big)\right) = \prod_{i=1}^{r} \operatorname{tr} S\big(p_i^{\alpha_i}\big).$$

The result now follows immediately from (3.6). □

The following corollary of Theorem 3.5 appears to be novel, as we were unable to find it in our extensive search of the literature. In particular, although the magnitude of the following determinant is possible to conjecture based on numerical evidence, the sign of the determinant is determined by a rather complicated formula that seems difficult to arrive at using other means.

Corollary 3.7 *If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is the canonical factorization of n into distinct primes $p_1, p_2, \ldots, p_r$, then*

$$\det\left[c_{d_i}\left(\frac{n}{d_j}\right)\right]_{i,j=1}^{\tau(n)} = n^{\frac{\tau(n)}{2}}(-1)^{\sum_{i=1}^{r}\lfloor\frac{\alpha_i+1}{2}\rfloor\frac{\tau(n)}{\alpha_i+1}}, \tag{3.23}$$

where $\tau(n)$ denotes the number of positive divisors $d_1, d_2, \ldots, d_{\tau(n)}$ of n.

Proof Simply observe that

$$\begin{aligned}
\det\left[c_{d_i}\left(\frac{n}{d_j}\right)\right]_{i,j=1}^{\tau(n)} &= \det S(n) && \text{by (2.15)}\\
&= n^{\frac{\tau(n)}{2}} \det U(n) && \text{by (2.16)}\\
&= n^{\frac{\tau(n)}{2}} \det\left(\bigotimes_{i=1}^{r} U\left(p_i^{\alpha_i}\right)\right) && \text{by (3.21)}\\
&= n^{\frac{\tau(n)}{2}} \prod_{i=1}^{r}\left(\det U\left(p_i^{\alpha_i}\right)\right)^{\frac{\tau(n)}{\alpha_i+1}} && \text{by (3.12)}\\
&= n^{\frac{\tau(n)}{2}} \prod_{i=1}^{r}\left((-1)^{\lfloor\frac{\alpha_i+1}{2}\rfloor}\right)^{\frac{\tau(n)}{\alpha_i+1}} && \text{by (3.11)}\\
&= n^{\frac{\tau(n)}{2}}(-1)^{\sum_{i=1}^{r}\lfloor\frac{\alpha_i+1}{2}\rfloor\frac{\tau(n)}{\alpha_i+1}}. && \square
\end{aligned}$$

3.6 Reciprocity and von Sterneck's formula

Our next result requires no proof, for it follows immediately from (2.17) and the fact that $U = U^T$.

Theorem 3.8 (Reciprocity formula) *If d and d' are positive divisors of n, then*

$$c_d\left(\frac{n}{d'}\right)\phi(d') = c_{d'}\left(\frac{n}{d}\right)\phi(d). \tag{3.24}$$

Although we have been unable to find (3.24) in the literature, given the long and storied history of the Ramanujan sum, it is certainly possible that we are not the first to have discovered it. In fact, various other reciprocity formulas have also been discussed [30, 31]. For our purposes, the importance of (3.24) lies in the fact that it provides a one-line proof of the following important formula [20, Thm. 272], [43, Cor. 2.4], [57, p. 40].

Corollary 3.9 (von Sterneck's formula) *For* $n, x \in \mathbb{Z}$ *with* $n \geq 1$, *we have*

$$c_n(x) = \frac{\mu(\frac{n}{(n,x)})\phi(n)}{\phi(\frac{n}{(n,x)})}. \tag{3.25}$$

Proof Let $d' = n$ and $d = n/(n,x)$ in (3.24) and use (2.14). □

Let us make a few historical remarks concerning the preceding formula. The peculiar arithmetic function on the right-hand side of (3.25) is sometimes called *von Sterneck's function*. It was first studied by von Sterneck (1902) [63], independently of Ramanujan sums, which first rose to prominence with Ramanujan's seminal paper (1918) [53, Paper 21]. It has frequently been claimed that the fact that von Sterneck's function equals $c_n(x)$ was first observed by Hölder (1936) [24]. However, Peter van der Kamp was kind enough to inform us that Kluyver (1906) [36, p. 410] had already discovered the equality (3.25) some thirty years before Hölder's paper appeared.

Before proceeding, let us also remark that Corollary 3.2 follows immediately from von Sterneck's formula by setting $x = 1$ and $x = n$, respectively, in (3.25).

Corollary 3.10 *If* $n \geq 1$, *then*

$$\sum_{d|n, d'|n} c_d\left(\frac{n}{d'}\right) c_{d'}\left(\frac{n}{d}\right) = n\tau(n).$$

Proof Letting I denote the $\tau(n) \times \tau(n)$ identity matrix, it follows from (3.22) that

$$\tau(n) = \operatorname{tr} I = \operatorname{tr} U^*U = \sum_{i,j=1}^{\tau(n)} \left(\left[U(n)\right]_{i,j}\right)^2 = \sum_{d|n,d'|n} \frac{1}{n}\left(c_d\left(\frac{n}{d'}\right)\right)^2 \frac{\phi(d')}{\phi(d)}.$$

The desired formula now follows from (3.24). □

3.7 A mixed orthogonality relation

An immediate consequence of Theorem 3.5 is the following orthogonality relation in which the parameters d and d' play quite different roles. The text [43, Thm. 2.8] devotes almost two pages to its proof.

Theorem 3.11 (Mixed orthogonality relation) *If* $n \geq 1$, $d|n$, *and* $d'|n$, *then*

$$\frac{1}{n}\sum_{k|n} c_d\left(\frac{n}{k}\right) c_k\left(\frac{n}{d'}\right) = \delta_{d,d'}. \tag{3.26}$$

Proof Compute the (i,j) entry in the equation $S(n)^2 = nI$. □

Corollary 3.12 *If x is an integer, then*

$$\sum_{k|n} c_k(x) = \begin{cases} n & \text{if } n|x, \\ 0 & \text{if } n \nmid x. \end{cases} \tag{3.27}$$

Proof Set $d = 1$ and $d' = n/(x,n)$ in (3.26) to obtain $\sum_{k|n} c_k((x,n)) = n\delta_{\frac{n}{(x,n)},1}$. Now apply (2.14) to obtain (3.27). □

Corollary 3.13 *If $n \geq 1$ and $d|n$, then*

$$\sum_{k|n} c_d\left(\frac{n}{k}\right)\mu(k) = \begin{cases} n & \text{if } d = n, \\ 0 & \text{if } d \neq n. \end{cases}$$

Proof Let $d' = n$ in (3.26) and use Corollary 3.2. □

One says that a function $f : \mathbb{Z} \to \mathbb{C}$ is *even modulo n* if

$$f\big((n,x)\big) = f(x)$$

for all integers x [43, p. 79], [57, p. 15]. As we noted in (2.14), since $c_n(x)$ is a superclass function with respect to the variable x, it follows that $c_n(x)$ is even modulo n. We remark that the following theorem [43, Thm. 2.9] has a trivial proof based upon supercharacter theory. In contrast, the standard proof requires several pages of straightforward but tedious manipulations.

Theorem 3.14 *If $f : \mathbb{Z} \to \mathbb{C}$ is an even function modulo n, then f can be written uniquely in the form*

$$f(x) = \sum_{d|n} \alpha(d) c_d(x), \tag{3.28}$$

where the coefficients $\alpha(d)$ are given by

$$\alpha(d) = \frac{1}{n}\sum_{k|n} f\left(\frac{n}{k}\right) c_k\left(\frac{n}{d}\right).$$

Proof Since the Ramanujan sums $c_{d_i}(x) = \sigma_i(x)$ form a basis for the space of all superclass functions by [14, Thm. 2.2], a unique expansion of the form (3.28) exists. The formula for the coefficients follows immediately from (3.26). □

As Hardy observes in the notes to [19, Paper 21], the following important result was first obtained by Kluyver (1906) [36, p. 410]. It also appears in the more recent texts [43, Prop. 2.1], [46, Thm. A.24], and [57, Thm. 3.1b].

Theorem 3.15 (Kluyver) *If $n, x \in \mathbb{Z}$ and $n \geq 1$, then*

$$c_n(x) = \sum_{d|(n,x)} \mu\left(\frac{n}{d}\right) d. \tag{3.29}$$

Proof Applying the Möbius inversion formula to (3.27), it follows that

$$c_n(x) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{k|d} c_k(x) = \sum_{d|n, d|x} \mu\left(\frac{n}{d}\right) d = \sum_{d|(n,x)} \mu\left(\frac{n}{d}\right) d. \qquad \square$$

Corollary 3.16 *For all $m, n \geq 1$, the inequality*

$$\left|c_n(m)\right| \leq \sigma(m)$$

holds. Here $\sigma(m)$ denotes the sum of the divisors of m.

4 Superclass arithmetic

In this section, we explore several further properties of Ramanujan sums that can be deduced by studying *superclass arithmetic* on $\mathbb{Z}/n\mathbb{Z}$. Although this approach has been attempted sporadically throughout the years [21, 34, 35, 42, 51], these earlier authors did not have the benefit of the general theory of supercharacters.

We state the following preparatory lemmas in full generality, noting that they apply to any finite group G (we require only the case $G = \mathbb{Z}/n\mathbb{Z}$). In fact, a more primitive approach was recently undertaken in [18], where Kloosterman sums were considered in the context of classical character theory.

4.1 Superclass constants and simultaneous diagonalization

Suppose that G is a finite group with supercharacter theory $(\mathcal{X}_H, \mathcal{K}_H)$ generated by the action of some subgroup H of $\mathrm{Aut}(G)$ (see Sect. 2.2). In particular, we obtain from the action of H on G a partition $\mathcal{X} = \{X_1, X_2, \ldots, X_r\}$ of $\mathrm{Irr}(G)$ with corresponding supercharacters (2.1) and a compatible partition $\mathcal{K} = \{K_1, K_2, \ldots, K_r\}$ of G into superclasses. We also note that the superclass sums

$$\hat{K}_i = \sum_{g \in K_i} g$$

belong to the center $\mathbf{Z}(\mathbb{C}[G])$ of the group algebra $\mathbb{C}[G]$. Indeed, each K_i is a union of conjugacy classes of G and it is well known that the corresponding class sums each belong to $\mathbf{Z}(\mathbb{C}[G])$ [26, Thm. 2.4].

Although the following lemma is a special case of [14, Cor. 2.3], we provide a brief explanation for the sake of completeness. Since we are, for the moment, working under the assumption that G is an arbitrary finite group, we write the group operation *multiplicatively*. When we later apply the following two results to $\mathbb{Z}/n\mathbb{Z}$, the group operation will be *addition* modulo n.

Lemma 4.1 *Fix some element z in K_k and let $a_{i,j,k}$ denote the number of solutions $(x_i, y_j) \in K_i \times K_j$ to the equation $xy = z$. The* superclass constants $a_{i,j,k}$ *satisfy*

$$\hat{K}_i \hat{K}_j = \sum_{k=1}^{r} a_{i,j,k} \hat{K}_k \tag{4.1}$$

for $1 \leq i, j, k \leq r$.

Proof It suffices to prove that $a_{i,j,k}$ does not depend upon the particular chosen representative z of K_k. Suppose that z_1 and z_2 belong to K_k. By the definition of the supercharacter theory $(\mathcal{X}_H, \mathcal{K}_H)$, there exists an automorphism $\varphi : G \to G$ belonging to H and an element g of G such that

$$\varphi(z_1) = \varphi(g)^{-1} z_2 \varphi(g).$$

If $(x_1, y_1) \in K_i \times K_j$ is a solution to the equation $xy = z_1$, then

$$\varphi(x_1)\varphi(y_1) = \varphi(z_1) = \varphi(g)^{-1} z_2 \varphi(g),$$

from which it follows that the elements $x_2 = \varphi(g x_1 g^{-1})$ of K_i and $y_2 = \varphi(g y_1 g^{-1})$ of K_j satisfy $x_2 y_2 = z_2$. Thus there is a bijection between solutions $(x_1, y_1) \in K_i \times K_j$ of $xy = z_1$ and solutions $(x_2, y_2) \in K_i \times K_j$ of $xy = z_2$. □

The following theorem is partly inspired by the corresponding result from classical character theory [13, Sect. 33], [18, Lem. 3.1], [38, Lem. 4]. Since we require a supercharacter version of this result, we provide a detailed proof. As with the preceding lemma, we work with an arbitrary finite group G, maintaining the notation and conventions established at the beginning of this subsection.

Theorem 4.2 *Let $M_i = (a_{i,j,k})_{j,k=1}^r$. If $W = (w_{j,k})_{j,k=1}^r$ denotes the $r \times r$ matrix with entries*

$$w_{j,k} = \frac{|K_j| \sigma_k(K_j)}{\sum_{\chi \in X_k} \chi(1)}, \tag{4.2}$$

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

$$M_i W = W D_i \tag{4.3}$$

for $i = 1, 2, \ldots, r$. In particular, the matrices $M_1, M_2, \ldots, M_r$ are simultaneously diagonalizable and commute with each other.

Proof Applying σ_k to the superclass sum $\hat{K}_j$, we first note that

$$\sigma_k(\hat{K}_j) = |K_j| \sigma_k(K_j) \tag{4.4}$$

since σ_k is a superclass function that assumes the constant value $\sigma_k(K_j)$ on the superclass K_j. Next let π_k be the matrix representation of G given by

$$\pi_k = \bigoplus_{\chi \in X_k} \chi(1) \pi_\chi, \tag{4.5}$$

where π_χ is an irreducible matrix representation whose character χ belongs to X_k. Since each $\hat{K}_j$ belongs to $\mathbf{Z}(\mathbb{C}[G])$ and each π_χ is irreducible, there exist constants $w_{j,k}^\chi$ such that

$$\pi_\chi(\hat{K}_j) = \frac{w_{j,k}^\chi}{\chi(1)} I_{\chi(1)}, \tag{4.6}$$

where $I_{\chi(1)}$ denotes the $\chi(1) \times \chi(1)$ identity matrix. Taking the trace of both sides of the preceding equation, we find that

$$\chi(\hat{K}_j) = w_{j,k}^{\chi}. \tag{4.7}$$

We now claim that $w_{j,k}^{\chi}$ is independent of which particular irreducible character χ in X_k is chosen. Indeed, if χ and χ' belong to X_k, then there exists an automorphism $\varphi : G \to G$ belonging to H such that $\chi = \chi' \circ \varphi$. Therefore,

$$\chi(\hat{K}_j) = \sum_{g \in K_j} \chi(g) = \sum_{g \in K_j} \chi'\big(\varphi(g)\big) = \sum_{h \in \varphi(K_j)} \chi'(h) = \sum_{h \in K_j} \chi'(h) = \chi'(\hat{K}_j)$$

since φ permutes the conjugacy classes that constitute the superclass K_j. In the following, we now write $w_{j,k}$ in place of $w_{j,k}^{\chi}$.

Substituting (4.6) into (4.5), we find that

$$\pi_k(\hat{K}_j) = \bigoplus_{\chi \in X_k} w_{j,k} I_{\chi(1)}. \tag{4.8}$$

Taking the trace of the preceding yields

$$\operatorname{tr} \pi_k(\hat{K}_j) = \sum_{\chi \in X_k} \chi(1) w_{j,k} = \sum_{\chi \in X_k} \chi(1)\chi(\hat{K}_j) = \sigma_k(\hat{K}_j)$$

by the definition (2.1) of the supercharacter σ_k. Returning to (4.4) and using the preceding, we find that

$$|K_j| \sigma_k(K_j) = \sigma_k(\hat{K}_j) = w_{j,k} \sum_{\chi \in X_k} \chi(1),$$

from which we obtain the desired formula (4.2) for $w_{j,k}$.

We now need to verify that the simultaneous diagonalization (4.3) holds. Applying π_ℓ to (4.1) and using (4.8), we see that

$$\left(\bigoplus_{\chi \in X_\ell} w_{i,\ell} I_{\chi(1)} \right) \left(\bigoplus_{\chi \in X_\ell} w_{j,\ell} I_{\chi(1)} \right) = \sum_{k=1}^{r} a_{i,j,k} \left(\bigoplus_{\chi \in X_\ell} w_{k,\ell} I_{\chi(1)} \right).$$

Considering the direct summand corresponding to an arbitrary χ in X_ℓ, we see that

$$w_{i,\ell} I_{\chi(1)} w_{j,\ell} I_{\chi(1)} = \sum_{k=1}^{r} a_{i,j,k} w_{k,\ell} I_{\chi(1)},$$

which in turn implies that

$$\sum_{k=1}^{r} a_{i,j,k} w_{k,\ell} = w_{j,\ell} w_{i,\ell}.$$

To conclude the proof, we observe that the preceding equation is simply the (j, ℓ) entry of the matrix equation (4.3). $\square$

4.2 The matrices $M_i(p^\alpha)$

We are now ready to discuss the matrices $M_i = M_i(n)$, as defined in Theorem 4.2, which arise from the supercharacter theory for $G = \mathbb{Z}/n\mathbb{Z}$ induced by $H = \mathrm{Aut}(G)$ (described in Sect. 2.2). We do this first for prime powers $n = p^\alpha$.

Let us first note that the divisors of p^α are the $\alpha + 1$ numbers $d_i = p^{i-1}$ for $i = 1, 2, \ldots, \alpha + 1$. In light of (2.12), this yields the corresponding superclasses

$$K_i = \bigl\{a \in \mathbb{Z}/p^\alpha\mathbb{Z} : \bigl(a, p^\alpha\bigr) = p^{\alpha-i+1}\bigr\} = \bigl\{xp^{\alpha-i+1} \in \mathbb{Z}/p^\alpha\mathbb{Z} : p \nmid x\bigr\}, \tag{4.9}$$

each of which satisfies

$$|K_i| = \phi\bigl(p^{i-1}\bigr)$$

by (2.13). Fixing some z in K_k, we let $a_{i,j,k}$ denote the number of solutions (x, y) in $K_i \times K_j$ to the equation

$$x + y = z. \tag{4.10}$$

Recall that since Lemma 4.1 concerns general groups, the corresponding equation $xy = z$ was written in multiplicative notation. However, since we are considering only abelian groups, we choose now to employ additive notation.

We claim that the matrix $M_i(p^\alpha) = [a_{i,j,k}]_{j,k=1}^{\alpha+1}$ is given by

$$\left[\begin{array}{cccc|c|cccc}
0 & 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 & \phi(p) & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & \phi(p^{i-2}) & 0 & 0 & \cdots & 0 \\
\hline
\phi(p^{i-1}) & \phi(p^{i-1}) & \cdots & \phi(p^{i-1}) & p^{i-1} - 2p^{i-2} & 0 & 0 & \cdots & 0 \\
\hline
0 & 0 & \cdots & 0 & 0 & \phi(p^{i-1}) & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 & 0 & 0 & \phi(p^{i-1}) & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & \phi(p^{i-1})
\end{array}\right], \tag{4.11}$$

where the ith row and column of M_i are singled out. Although the computations involved are elementary, we feel compelled to provide a complete justification of (4.11) since so many of our upcoming results depend upon this formula. The reader is invited to consult Appendix for the details.

The matrix $W = W(p^\alpha)$ described by Theorem 4.2 is somewhat easier to describe. In fact, we claim that

$$W\bigl(p^\alpha\bigr) = S\bigl(p^\alpha\bigr), \tag{4.12}$$

the supercharacter table for $\mathbb{Z}/p^\alpha\mathbb{Z}$ discussed in Sect. 3.1. To see this, simply note that

$$\begin{aligned}
\big[W\big(p^\alpha\big)\big]_{j,k} &= \frac{|K_j|\sigma_k(K_j)}{\sum_{\chi\in X_k}\chi(1)} && \text{by (4.2)}\\
&= \frac{\phi(d_j)c_{d_k}(\frac{n}{d_j})}{\phi(d_k)} && \text{by (2.10), (2.11), (2.13)}\\
&= c_{d_j}\left(\frac{n}{d_k}\right). && \text{by (3.24)}
\end{aligned}$$

Finally, there are the diagonal matrices $D_i = D_i(p^\alpha)$. By Theorem 4.2 we have

$$\big[D_i\big(p^\alpha\big)\big]_{j,k} = \delta_{j,k}c_{d_i}\left(\frac{p^\alpha}{d_k}\right) = \delta_{j,k}c_{p^{i-1}}\big(p^{\alpha-k+1}\big). \tag{4.13}$$

Example 4 The case $p=3$ and $\alpha=4$ yields the divisors $d_1=1$, $d_2=3$, $d_3=9$, $d_4=27$, and $d_5=81$ of $p^\alpha=81$. The corresponding matrices M_1, M_2, M_3, M_4, M_5 are displayed below.

$$\underbrace{\left[\begin{array}{c|cccc}
1 & 0 & 0 & 0 & 0\\ \hline
0 & 1 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 1
\end{array}\right]}_{M_1}
\quad
\underbrace{\left[\begin{array}{c|c|ccc}
0 & 1 & 0 & 0 & 0\\ \hline
2 & 1 & 0 & 0 & 0\\ \hline
0 & 0 & 2 & 0 & 0\\
0 & 0 & 0 & 2 & 0\\
0 & 0 & 0 & 0 & 2
\end{array}\right]}_{M_2}
\quad
\underbrace{\left[\begin{array}{cc|c|cc}
0 & 0 & 1 & 0 & 0\\
0 & 0 & 2 & 0 & 0\\ \hline
6 & 6 & 3 & 0 & 0\\ \hline
0 & 0 & 0 & 6 & 0\\
0 & 0 & 0 & 0 & 6
\end{array}\right]}_{M_3}$$

$$\underbrace{\left[\begin{array}{ccc|c|c}
0 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 2 & 0\\
0 & 0 & 0 & 6 & 0\\ \hline
18 & 18 & 18 & 9 & 0\\ \hline
0 & 0 & 0 & 0 & 18
\end{array}\right]}_{M_4}
\quad
\underbrace{\left[\begin{array}{cccc|c}
0 & 0 & 0 & 0 & 1\\
0 & 0 & 0 & 0 & 2\\
0 & 0 & 0 & 0 & 6\\
0 & 0 & 0 & 0 & 18\\ \hline
54 & 54 & 54 & 54 & 27
\end{array}\right]}_{M_5}.$$

These matrices each satisfy $M_iW = WD_i$ where

$$W = \begin{bmatrix}
1 & 1 & 1 & 1 & 1\\
2 & 2 & 2 & 2 & -1\\
6 & 6 & 6 & -3 & 0\\
18 & 18 & -9 & 0 & 0\\
54 & -27 & 0 & 0 & 0
\end{bmatrix}$$

is the supercharacter table $S(81)$ and

$$D_1 = \operatorname{diag}(1,1,1,1,1),$$

$$D_2 = \operatorname{diag}(2,2,2,2,-1),$$

$$\begin{aligned}D_3 &= \operatorname{diag}(6, 6, 6, -3, 0),\\ D_4 &= \operatorname{diag}(18, 18, -9, 0, 0),\\ D_5 &= \operatorname{diag}(54, 27, 0, 0, 0).\end{aligned}$$

Before proceeding, let us make a few remarks about the matrices (4.11). First observe that $M_i(p^\alpha)$ is a multiple of a stochastic matrix since each column of $M_i(p^\alpha)$ sums to $\phi(p^{i-1})$. Indeed, we only need verify this for the ith column of $M_i(p^\alpha)$:

$$\begin{aligned}&1+\phi(p)+\phi\bigl(p^2\bigr)+\cdots+\phi\bigl(p^{i-2}\bigr)+\bigl(p^{i-1}-2p^{i-2}\bigr)\\ &\quad= 1+(p-1)+\bigl(p^2-p\bigr)+\cdots+\bigl(p^{i-2}-p^{i-3}\bigr)+\bigl(p^{i-1}-2p^{i-2}\bigr)\\ &\quad= p^{i-1}-p^{i-2}\\ &\quad= \phi\bigl(p^{i-1}\bigr).\end{aligned}$$

Let us also note that

$$\sum_{i=1}^{\alpha+1} M_i\bigl(p^\alpha\bigr)=\begin{bmatrix} 1 & 1 & \cdots & 1\\ \phi(p) & \phi(p) & \cdots & \phi(p)\\ \vdots & \vdots & \ddots & \vdots\\ \phi(p^\alpha) & \phi(p^\alpha) & \cdots & \phi(p^\alpha)\end{bmatrix}. \tag{4.14}$$

This can be deduced from (4.11) and the fact that for $j \neq k$, the corresponding off-diagonal matrix entry $[M_i(p^\alpha)]_{j,k}$ is nonzero for only a single value of i. Finally, we observe that

$$1 \le i < j \le \alpha+1 \quad\Longrightarrow\quad M_iM_j=\phi\bigl(p^{i-1}\bigr)M_j=M_jM_i \tag{4.15}$$

follows from a straightforward computation.

4.3 The matrices $M_i(n)$ for general n

Having computed the matrices $M_i(p^\alpha)$ for prime powers, we now turn to the problem of computing $M_i(n)$ for general n and harnessing the power of Theorem 4.2 to produce new identities for Ramanujan sums. The approach is straightforward enough, for the simultaneous diagonalization (4.3) "tensors" in the expected manner, much as the supercharacter tables did in Theorem 3.5. The difficulty in establishing this is mostly notational. We therefore take a moment to introduce the somewhat elaborate notation which is required.

Suppose that $(m,n)=1$ and let $d_1, d_2, \ldots, d_{\tau(m)}$ and $e_1, e_2, \ldots, e_{\tau(n)}$ be ordered lists of the divisors of m and n, respectively. Having specified an order to the divisors of m and n, we can generate the matrices $M_i(m)$, $W(m)$, $D_i(m)$ and $M_{i'}(n)$, $W(n)$, $D_{i'}(n)$, respectively, as defined by Theorem 4.2 (i.e., apply Theorem 4.2 separately to the two groups $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$, each endowed with the supercharacter theory described in Sect. 2.2).

Next we observe that the divisors of mn are clearly the $\tau(mn)=\tau(m)\tau(n)$ numbers $d_ie_{i'}$ where $1 \le i \le \tau(m)$ and $1 \le i' \le \tau(n)$. However, we need the divisors of

mn to be listed in some specific linear order since such an ordering will allow us to label the corresponding superclasses and supercharacters on $\mathbb{Z}/mn\mathbb{Z}$. We therefore impose the lexicographic order on the set

$$\big\{d_i e_{i'} : 1 \le i \le \tau(m), 1 \le i' \le \tau(n)\big\}$$

of divisors of mn that is induced by the lexicographic ordering of the Cartesian product $\{1, 2, \dots, \tau(m)\} \times \{1, 2, \dots, \tau(n)\}$. This gives rise to an order-preserving bijection

$$\sigma : \big\{1, 2, \dots, \tau(m)\big\} \times \big\{1, 2, \dots, \tau(n)\big\} \to \big\{1, 2, \dots, \tau(mn)\big\},$$

which implicitly provides us with an ordered list of the divisors of mn. We now consider the matrices $M_1(mn), M_2(mn), \dots, M_{\tau(mn)}(mn)$, the diagonal matrices $D_1(mn), D_2(mn), \dots, D_{\tau(mn)}(mn)$, and the matrix $W(mn)$ that intertwines them.

Lemma 4.3 *Maintaining the notation and conventions described above,*

$$\big[M_{\sigma(i,i')}(mn)\big]_{\sigma(j,j'),\sigma(k,k')} = \big[M_i(m)\big]_{j,k}\big[M_{i'}(n)\big]_{j',k'}, \tag{4.16}$$

$$\big[D_{\sigma(i,i')}(mn)\big]_{\sigma(j,j'),\sigma(k,k')} = \big[D_i(m)\big]_{j,k}\big[D_{i'}(n)\big]_{j',k'}, \tag{4.17}$$

$$\big[W(mn)\big]_{\sigma(j,j'),\sigma(k,k')} = \big[W(m)\big]_{j,k}\big[W(n)\big]_{j',k'}, \tag{4.18}$$

for all $1 \le i, j, k \le \tau(m)$ *and* $1 \le i', j', k' \le \tau(n)$. *In other words, the simultaneous diagonalization* (4.3) *of Theorem* 4.2 *is compatible with Kronecker products in the sense that*

$$\underbrace{\big(M_i(m) \otimes M_{i'}(n)\big)}_{M_{\sigma(i,i')}(mn)}\underbrace{\big(W(m) \otimes W(n)\big)}_{W(mn)} = \underbrace{\big(W(m) \otimes W(n)\big)}_{W(mn)}\underbrace{\big(D_i(m) \otimes D_{i'}(n)\big)}_{D_{\sigma(i,i')(mn)}}$$

whenever $(m, n) = 1$. *In particular,* $W(mn) = S(mn)$, *the corresponding supercharacter table for* $\mathbb{Z}/mn\mathbb{Z}$.

Proof The given lists $d_1, d_2, \dots, d_{\tau(m)}$ and $e_1, e_2, \dots, e_{\tau(n)}$ provide us with corresponding superclasses

$$K_i(m) = \left\{a \in \mathbb{Z}/m\mathbb{Z} : (a, m) = \frac{m}{d_i}\right\}, \qquad K_{i'}(n) = \left\{b \in \mathbb{Z}/n\mathbb{Z} : (b, n) = \frac{n}{e_{i'}}\right\},$$

in $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$. For each pair (i, i') satisfying $1 \le i \le \tau(m)$ and $1 \le i' \le \tau(n)$, we define

$$K_{\sigma(i,i')}(mn) = \left\{c \in \mathbb{Z}/mn\mathbb{Z} : (c, mn) = \frac{mn}{d_i e_{i'}}\right\},$$

yielding a partition of $\mathbb{Z}/mn\mathbb{Z}$ into $\tau(m)\tau(n) = \tau(mn)$ superclasses. By the Chinese Remainder Theorem, the map $\Phi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z}$ defined by $\Phi((a,b)) = ab \pmod{mn}$ is a ring isomorphism that satisfies

$$\Phi\big(K_i(m) \times K_{i'}(n)\big) = K_{\sigma(i,i')}(mn). \tag{4.19}$$

Fix elements z, z' in $K_k(m)$ and $K_{k'}(n)$, respectively, and let

$$a_{i,j,k}(m) = \big|\big\{(x,y) \in K_i(m) \times K_j(m) : x + y = z\big\}\big|,$$
$$a_{i',j',k'}(n) = \big|\big\{\big(x',y'\big) \in K_{i'}(n) \times K_{j'}(n) : x' + y' = z'\big\}\big|.$$

Clearly the product $a_{i,j,k}(m)a_{i',j',k'}(n)$ equals the number of solutions to

$$\big(x,x'\big) + \big(y,y'\big) = \big(z,z'\big),$$

where (x,x') belongs to $K_i(m) \times K_{i'}(n)$, and (y,y') belongs to $K_j(m) \times K_{j'}(n)$. Applying Φ to both sides of the preceding and using (4.19), it follows that $a_{i,j,k}(m)a_{i',j',k'}(n)$ equals the number of solutions to $X + Y = Z$ where $Z = \Phi(z,z')$ is a fixed element of $K_{\sigma(k,k')}(mn)$, X belongs to $K_{\sigma(i,i')}(mn)$, and Y belongs to $K_{\sigma(j,j')}(mn)$, respectively. In other words,

$$a_{\sigma(i,i'),\sigma(j,j'),\sigma(k,k')}(mn) = a_{i,j,k}(m)a_{i',j',k'}(n), \tag{4.20}$$

so that

$$\big[M_{\sigma(i,i')}(mn)\big]_{\sigma(j,j'),\sigma(k,k')} = \big[M_i(m)\big]_{j,k}\big[M_{i'}(n)\big]_{j',k'}.$$

This establishes (4.16).

Turning our attention to (4.17), we recall from Theorem 4.2 that the matrix $D_{\sigma(i,i')}(mn)$ is diagonal. In fact, its diagonal entries are precisely

$$\begin{aligned}
\big[D_{\sigma(i,i')}(mn)\big]_{\sigma(j,j'),\sigma(j,j')} &= \frac{|K_{\sigma(i,i')}(mn)|c_{d_je_{j'}}(\frac{mn}{d_ie_{i'}})}{|K_{\sigma(j,j')}(mn)|} && \text{by (4.2), (2.11)}\\
&= \frac{|K_i(m)||K_{i'}(n)|c_{d_j}(\frac{m}{d_i})c_{e_{j'}}(\frac{n}{e_{i'}})}{|K_j(m)||K_{j'}(n)|} && \text{by (4.19), (3.20)}\\
&= \frac{|K_i(m)|c_{d_j}(\frac{m}{d_i})}{|K_j(m)|}\cdot\frac{|K_{i'}(n)|c_{e_{j'}}(\frac{n}{d_{i'}})}{|K_{j'}(n)|}\\
&= \big[D_i(m)\big]_{j,j}\big[D_{i'}(n)\big]_{j',j'}. && \text{by (4.2)}
\end{aligned}$$

The proof of (4.18) is similar, and in fact much easier, since $W(m)$, $W(n)$, and $W(mn)$ do not depend upon the indices i, i'. The fact that $W(mn) = S(mn)$ follows immediately from (4.12) and (3.21). □

Our primary interest in the preceding lemma lies in the following straightforward generalization. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ denote the factorization of n into distinct primes, and let $d_1, d_2, \ldots, d_{\tau(n)}$ denote the divisors of n. Noting that

$$\tau(n) = \prod_{\ell=1}^{r} (\alpha_\ell + 1),$$

we let

$$\sigma : \prod_{\ell=1}^{r} \{1, 2, \ldots, \alpha_\ell + 1\} \to \big\{1, 2, \ldots, \tau(n)\big\}$$

be a bijection that preserves the lexicographic order on the Cartesian product $\prod_{\ell=1}^{r} \{1, 2, \ldots, \alpha_\ell + 1\}$. According to this labeling scheme,

$$d_{\sigma(i_1, i_2, \ldots, i_r)} = p_1^{i_1 - 1} p_2^{i_2 - 1} \cdots p_r^{i_r - 1} \tag{4.21}$$

is the $\sigma(i_1, i_2, \ldots, i_r)$th divisor of n. In light of Lemma 4.3, it follows that

$$D_{\sigma(i_1, i_2, \ldots, i_r)}(n) \cong \bigotimes_{\ell=1}^{r} D_{i_\ell}\big(p_\ell^{\alpha_\ell}\big) \sim \bigotimes_{\ell=1}^{r} M_{i_\ell}\big(p_\ell^{\alpha_\ell}\big) \cong M_{\sigma(i_1, i_2, \ldots, i_r)}(n), \tag{4.22}$$

where $\sim$ denotes similarity, and $\cong$ denotes similarity by a permutation matrix. In particular, the eigenvalues of the diagonal matrix $D_{\sigma(i_1, i_2, \ldots, i_r)}(n)$ are precisely the $\tau(n)$ numbers

$$c_{d_{\sigma(i_1, i_2, \ldots, i_r)}}(d_j)$$

for $j = 1, 2, \ldots, \tau(n)$. We can therefore obtain from (4.22) a variety of formulas involving Ramanujan sums by utilizing the detailed information about the matrices $M_{i_\ell}(p_\ell^{\alpha_\ell})$ we derived in Sect. 4.2.

4.4 Ramanujan sums and superclass constants

Fix a positive integer n and let $a_{i,j,k} = a_{i,j,k}(n)$, $M_i = M_i(n)$, and so forth. Now let us observe that

$$\begin{aligned}
M_i &= W D_i W^{-1} && \text{by Theorem 4.2} \\
&= S D_i S^{-1} && \text{by Lemma 4.3} \\
&= \frac{1}{n} S D_i S. && \text{by Theorem 3.5}
\end{aligned}$$

Comparing the (j, k) entry in the equality $n M_i = S D_i S$ yields the formula

$$n a_{i,j,k} = \sum_{d|n} c_{d_i}(d) c_{d_j}(d) c_{\frac{n}{d}}\left(\frac{n}{d_k}\right).$$

In light of (3.24), we may rewrite the preceding in the more symmetric form

$$n \phi(d_k) a_{i,j,k} = \sum_{d|n} \phi\left(\frac{n}{d}\right) c_{d_i}(d) c_{d_j}(d) c_{d_k}(d). \tag{4.23}$$

Since the right side of (4.23) is symmetric in i, j, k, it follows that $\phi(d_k)a_{i,j,k} = \phi(d_j)a_{k,i,j}$. By definition, the superclass constants satisfy $a_{k,i,j} = a_{i,k,j}$, whence

$$\phi(d_k)a_{i,j,k} = \phi(d_j)a_{i,k,j}. \tag{4.24}$$

Indeed, this pattern is evident in the structure (4.11) of the matrices $M_i(p^\alpha)$. Another consequence of (4.23) is the following result.

Theorem 4.4 *If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is the canonical factorization of n into distinct primes $p_1, p_2, \ldots, p_r$ and $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ is a divisor of n, then*

$$\sum_{d'|n} \phi\left(\frac{n}{d'}\right)\left(c_d(d')\right)^3 = \begin{cases} 0 & \text{if } 2|d, \\ n\phi(d)\prod_{\ell=1}^r \lceil p_\ell^{\beta_\ell} - 2p_\ell^{\beta_\ell - 1}\rceil & \text{if } 2\nmid d, \end{cases} \tag{4.25}$$

where $\lceil \cdot \rceil$ denotes the ceiling function.

Proof By Corollary 3.4 and the multiplicativity of the Euler totient function, it suffices to establish the desired identity when $n = p^\alpha$ is a prime power. Let $d = d_i = p^{i-1}$ and recall from (4.11) that $a_{i,i,i}(p^\alpha) = 1$ if $i = 1$ and $a_{i,i,i}(p^\alpha) = p^{i-1} - 2p^{i-2}$ otherwise. Setting $i = j = k$ in (4.23), we obtain (4.25) for $n = p^\alpha$. □

4.5 Power sum identities

The preceding material now allows us to rapidly produce a wide variety of power sum identities involving Ramanujan sums, all of which appear to be novel. This highlights our larger argument, namely that supercharacter theory and superclass arithmetic are powerful tools, which can yield new insights, even when applied to the most elementary of groups (i.e., the cyclic groups $\mathbb{Z}/n\mathbb{Z}$).

Theorem 4.5 *If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is the canonical factorization of n into distinct primes $p_1, p_2, \ldots, p_r$ and $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ is a divisor of n, then for $s = 0, 1, 2, \ldots,$ we have*

$$\sum_{k|n} \left(c_d(k)\right)^s = \prod_{\ell=1}^r \left((\alpha_\ell - \beta_\ell + 1)\phi\left(p_\ell^{\beta_\ell}\right)^s + (-1)^s \lfloor p_\ell^{\beta_\ell - 1}\rfloor^s\right).$$

Here $\lfloor \cdot \rfloor$ denotes the floor function.

Proof By Corollary 3.4 it suffices to establish the desired formula when $n = p^\alpha$ is a prime power. Recall from (4.11) that for $2 \le i \le \alpha + 1$, we have

$$M_i\left(p^\alpha\right) = \begin{bmatrix} 0 & \mathbf{b} \\ \mathbf{c} & x \end{bmatrix} \oplus \phi\left(p^{i-1}\right) I_{\alpha - i + 1}, \tag{4.26}$$

where $\mathbf{b}$ and $\mathbf{c}$ are certain $(i-1) \times 1$ and $1 \times (i-1)$ matrices that satisfy

$$\mathbf{cb} = \phi\left(p^{i-1}\right)\left(1 + (p-1) + \left(p^2 - p\right) + \cdots + \left(p^{i-2} - p^{i-3}\right)\right) = \phi\left(p^{i-1}\right)p^{i-2},$$

and where $x = p^{i-1} - 2p^{i-2}$. A short inductive argument confirms that for each $s = 0, 1, 2, \ldots$, there exist corresponding polynomials $f_{11}, f_{12}, f_{21}, f_{22}$ such that

$$\begin{bmatrix} 0 & \mathbf{b} \\ \mathbf{c} & x \end{bmatrix}^s = \begin{bmatrix} f_{11}(\mathbf{bc}) & f_{12}(\mathbf{bc})\mathbf{b} \\ \mathbf{c} f_{21}(\mathbf{bc}) & f_{22}(\mathbf{cb}) \end{bmatrix}. \tag{4.27}$$

In particular, note that the preceding formula also holds when $\mathbf{b}$ and $\mathbf{c}$ are replaced by positive real numbers b and c and when the matrices involved are regarded simply as 2×2 matrices with real entries. Letting $b, c > 0$ satisfy

$$cb = \mathbf{cb} = \phi\big(p^{i-1}\big)p^{i-2}, \tag{4.28}$$

it follows from (4.27) and an elementary diagonalization argument that

$$\begin{aligned}
\operatorname{tr} \begin{bmatrix} 0 & \mathbf{b} \\ \mathbf{c} & x \end{bmatrix}^s &= \operatorname{tr} f_{11}(\mathbf{bc}) + \operatorname{tr} f_{22}(\mathbf{cb}) \\
&= \operatorname{tr} f_{11}(\mathbf{cb}) + \operatorname{tr} f_{22}(\mathbf{cb}) \\
&= \operatorname{tr} f_{11}(cb) + \operatorname{tr} f_{22}(cb) \\
&= \operatorname{tr} \begin{bmatrix} 0 & b \\ c & x \end{bmatrix}^s \\
&= \left(\frac{x + \sqrt{4bc + x^2}}{2} \right)^s + \left(\frac{x - \sqrt{4bc + x^2}}{2} \right)^s \\
&= \left[\frac{(p^{i-1} - 2p^{i-2}) + p^{i-1}}{2} \right]^s + \left[\frac{(p^{i-1} - 2p^{i-2}) - p^{i-1}}{2} \right]^s \\
&= \big(p^{i-1} - p^{i-2}\big)^s + \big(-p^{i-2}\big)^s \\
&= \phi\big(p^{i-1}\big)^s + \big(-p^{i-2}\big)^s.
\end{aligned}$$

Returning to (4.26), we find that

$$\operatorname{tr} M_i^s\big(p^\alpha\big) = (\alpha - i + 2)\phi\big(p^{i-1}\big)^s + \big(-p^{i-2}\big)^s \tag{4.29}$$

when $2 \le i \le \alpha + 1$. Since $M_1(p^\alpha)$ is the $(\alpha + 1) \times (\alpha + 1)$ identity matrix, setting $\beta = i - 1$, it follows that

$$\begin{aligned}
\sum_{k \mid p^\alpha} \big(c_{p^\beta}(k)\big)^s &= \operatorname{tr} D_{\beta+1}^s\big(p^\alpha\big) && \text{by (4.13)} \\
&= \operatorname{tr} M_{\beta+1}^s\big(p^\alpha\big) && \text{by Theorem 4.2} \\
&= (\alpha - \beta + 1)\phi\big(p^\beta\big)^s + (-1)^s \big\lfloor p^{\beta-1} \big\rfloor^s, && \text{by (4.29)}
\end{aligned}$$

as required. $\square$

In light of (4.15), it is not hard to generate more complicated variants of the preceding formula. For instance, since

$$\operatorname{tr} M_i^s\big(p^\alpha\big)M_j^s\big(p^\alpha\big)=\begin{cases}\phi(p^{i-1})^s \operatorname{tr} M_j^s(p^\alpha) & \text{if } i<j,\\ \operatorname{tr} M_i^{2s}(p^\alpha) & \text{if } i=j,\\ \phi(p^{j-1})^s \operatorname{tr} M_i^s(p^\alpha) & \text{if } i>j,\end{cases}$$

the quantity $\operatorname{tr} M_i^s(p^\alpha)M_j^s(p^\alpha)$ can be evaluated using similar methods. A little algebra then yields the following generalization of Theorem 4.5.

Theorem 4.6 *Let $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ be the canonical factorization of n into distinct primes $p_1,p_2,\dots,p_r$. If $d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r}$ and $d'=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_r^{\gamma_r}$ are divisors of n, then for $s=0,1,2,\dots$, we have*

$$\begin{aligned}&\sum_{k|n}\big(c_d(k)c_{d'}(k)\big)^s\\ &\quad=\prod_{\ell=1}^{r}\Big(\big(\alpha_\ell-\max\{\beta_\ell,\gamma_\ell\}+1\big)\phi\big(p_\ell^{\beta_\ell}\big)^s\phi\big(p_\ell^{\gamma_\ell}\big)^s\\ &\qquad+\big(\big\lfloor p^{\min\{\beta_\ell,\gamma_\ell\}-1}\big\rfloor-(1-\delta_{\beta_\ell,\gamma_\ell})p^{\min\{\beta_\ell,\gamma_\ell\}}\big)^s\big\lfloor p^{\max\{\beta_\ell,\gamma_\ell\}-1}\big\rfloor^s\Big),\end{aligned}$$

where δ denotes the Kronecker delta function.

Although it might at first appear that the preceding results could be adapted to handle negative exponents s, there are a few minor obstacles. First is the fact that $M_i(p^\alpha)$ is invertible if and only if $i=1$ or $i=2$. This corresponds to the fact that $c_d(k)$ vanishes for certain values of k if d is not square-free. Indeed, this can be seen directly from von Sterneck's formula (3.25) and the definition (3.2) of the Möbius μ-function. The correct adaptation of Theorem 4.5 for negative exponents is the following.

Theorem 4.7 *If $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ is the canonical factorization of n into distinct primes $p_1,p_2,\dots,p_r$ and $d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r}$ is a square-free divisor of n (i.e., $0\le\beta_i\le 1$ for $i=1,2,\dots,r$), then for $s=0,1,2,\dots$, we have*

$$\sum_{k|n}\frac{1}{(c_d(k))^s}=\prod_{\ell=1}^{r}\bigg(\frac{\alpha_\ell}{(p_\ell-1)^{\beta_\ell s}}+(-1)^{\beta_\ell s}\bigg).$$

Proof As before, it suffices to prove the desired formula when $n = p^\alpha$ is a prime power. The upper-left 2×2 submatrix of the $(\alpha+1) \times (\alpha+1)$ matrix

$$M_2(p^\alpha) = \left[\begin{array}{cc|cccc} 0 & 1 & 0 & 0 & \cdots & 0 \\ p-1 & p-2 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & p-1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & p-1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p-1 \end{array}\right]$$

has the eigenvalues -1 and $p-1$. On the other hand, $M_1(p^\alpha)$ is the identity matrix and hence has the eigenvalue 1 with multiplicity $\alpha+1$. Therefore,

$$\begin{aligned} \sum_{k|p^\alpha} \frac{1}{(c_{p^\beta}(k))^s} &= \operatorname{tr} D_{\beta+1}^{-s}(p^\alpha) && \text{by (4.13)} \\ &= \operatorname{tr} M_{\beta+1}^{-s}(p^\alpha) && \text{by Theorem 4.2} \\ &= \frac{\alpha}{(p-1)^{\beta s}} + (-1)^{\beta s}, \end{aligned}$$

as required. □

Along similar lines, we have the following.

Theorem 4.8 *If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is the canonical factorization of n into distinct primes $p_1, p_2, \ldots, p_r$ and $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ is a square-free divisor of n (i.e., $0 \le \beta_i \le 1$ for $i = 1, 2, \ldots, r$), then for z in $\mathbb{C}$, we have*

$$\sum_{k|n} \frac{1}{|c_d(k)|^z} = \prod_{\ell=1}^{r} \left(1 + \frac{\alpha_\ell}{(p_\ell - 1)^{\beta_\ell z}}\right). \tag{4.30}$$

Proof Noting that $|c_d(k)|^z = (c_d(k)^2)^{\frac{z}{2}}$ and that

$$\operatorname{tr}\left(M_{\beta+1}^2(p^\alpha)\right)^{-\frac{z}{2}} = 1 + \frac{\alpha}{(p-1)^{\beta z}},$$

the proof is similar to the proof of Theorem 4.5. □

Since the expression (4.30) bears some resemblance to the classical Riemann ζ-function and its variants, it is natural to ask whether this expression obeys the analogue of the Riemann hypothesis. The following result shows that this occurs if and only if n and d satisfy some rather peculiar hypotheses.

Corollary 4.9 *The complex roots of the function (4.30) all lie on the line $\Re z = \frac{1}{2}$ if and only if each prime p which divides d is of the form $\alpha^2 + 1$ where p^α is the highest power of p that divides n.*

Proof The complex roots of (4.30) are precisely the numbers

$$z = \frac{\log|\alpha_\ell| + i(2m+1)\pi}{\log(p_\ell - 1)}, \quad m \in \mathbb{Z},$$

for those ℓ such that $\beta_\ell = 1$ (i.e., for those primes p_ℓ that divide d). The real part of the preceding clearly equals $\frac{1}{2}$ if and only if $p_\ell = \alpha_\ell^2 + 1$. □

Example 5 Let $n = 5^2 \times 17^4 \times 37^6 = 5,357,300,885,152,225$ and $d = 5 \times 17 \times 37 = 3,145$. Since $5 = 2^2 + 1$, $17 = 4^2 + 1$, and $37 = 6^2 + 1$, it follows that the corresponding "ζ-function" (4.30) satisfies the Riemann hypothesis.

Using (4.15) and some of the preceding computations, it is not hard to explicitly evaluate the trace of any word composed using $M_1(p^\alpha), M_2(p^\alpha), \ldots, M_{\alpha+1}(p^\alpha)$, and $M_2(p^\alpha)^{-1}$. Consequently, the motivated individual could in principle provide an explicit formula for the sum

$$\sum_{k|n} \frac{c_{f_1}(k)^{s_1} c_{f_2}(k)^{s_2} \cdots c_{f_\eta}(k)^{s_\eta}}{c_{g_1}(k)^{t_1} c_{g_2}(k)^{t_2} \cdots c_{g_\nu}(k)^{t_\nu}},$$

where $f_1, f_2, \ldots, f_\eta$ are divisors of n, and $g_1, g_2, \ldots, g_\nu$ are square-free divisors of n. We make no attempt to do so here, having made our point that the arithmetic of superclasses can be used to deduce a variety of identities for Ramanujan sums.

5 Conclusion

We have demonstrated that reexamining even the most elementary of groups, namely the cyclic groups $\mathbb{Z}/n\mathbb{Z}$, from the perspective of supercharacter theory can yield surprising results. In particular, almost the entire algebraic theory of Ramanujan sums can be derived, in a systematic manner, using this approach. Many of the familiar classical identities for these fascinating sums, along with a variety of new ones, can be obtained with minimal effort once the basic machinery has been developed.

All of our results follow directly from a general theoretical framework without ad hoc arguments. More importantly, many of the ideas developed in this note can be applied to arbitrary finite groups. In particular, the arithmetic of superclasses (Sect. 4) and the simultaneous diagonalization theorem (Theorem 4.2), which yielded some of the more elaborate identities for Ramanujan sums, hold in much greater generality. We therefore hope that revisiting other families of elementary groups (e.g., dihedral groups, Frobenius groups, symmetric groups, p-groups,…) from the perspective of supercharacter theory might yield further information about other exponential sums (e.g., Gauss sums, Kloosterman sums, Jacobi sums, and their variants), which are of interest in number theory (see [10]).

Appendix: Computing the matrix $M_i(p^\alpha)$

This appendix contains a detailed derivation of the description (4.11) for the matrix $M_i(p^\alpha)$ given in Sect. 4.2.

The proof of Lemma 4.1 tells us that $a_{i,j,k}$ is independent of the particular chosen representative z of K_k. Since $\mathbb{Z}/p^\alpha\mathbb{Z}$ is abelian, we also note that

$$a_{i,j,k} = a_{j,i,k} \tag{A.1}$$

and

$$a_{i,j,k} = 0 \quad \Longleftrightarrow \quad a_{i,k,j} = 0. \tag{A.2}$$

Statement (A.2) requires some explanation. Observe that $a_{i,j,k} = 0$ holds if and only if $x + y = z$ has no solutions (x, y, z) in $K_i \times K_j \times K_k$. Since $K_j = -K_j$ and $K_k = -K_k$ by (4.9), it follows that the preceding happens if and only if $x + z' = y'$ has no solutions (x, z', y') in $K_i \times K_k \times K_j$. On the other hand, it is important to note that $a_{i,j,k} = a_{i,k,j}$ does not hold in general since the fixed representative z of K_k used in (4.10) plays a distinguished role.

We first break down the evaluation of the $a_{i,j,k}$ into five special cases, from which the structure of the matrix $M_i = M_i(p^\alpha)$ can eventually be deduced.

Lemma A.1 *For $G = \mathbb{Z}/p^\alpha\mathbb{Z}$ and $K_i = \{xp^{\alpha-i+1} \in \mathbb{Z}/p^\alpha\mathbb{Z} : p \nmid x\}$, we have*

(a) *if $k > i$ and $j \neq k$, then $a_{i,j,k} = 0$,*
(b) *if $j = k > i$, then $a_{i,j,k} = \phi(p^{i-1})$,*
(c) *if $j = k = i$, then $a_{i,j,k} = p^{i-1} - 2p^{i-2}$,*
(d) *if $j > k$ and $i \neq j$, then $a_{i,j,k} = 0$,*
(e) *if $i = j > k$, then $a_{i,j,k} = \phi(p^{i-1})$.*

Proof We first prove (a). Letting $k > i$ and $j \neq k$, we may assume that $i \leq j$ by (A.1). If $x_i = xp^{\alpha-i+1}$ and $y_j = yp^{\alpha-j+1}$ belong to K_i and K_j, respectively, then it follows that

$$x_i + y_j = p^{\alpha-j+1}\big(xp^{j-i} + y\big) \tag{A.3}$$

belongs to K_j since $xp^{j-i} + y$ is not divisible by p (recall that $p \nmid x$ and $p \nmid y$ by the definition of K_i and K_j). Since $j \neq k$, it follows from (A.3) that $x_i + y_j$ cannot belong to K_k, from which it follows that $a_{i,j,k} = 0$.

Next we consider (b). Suppose that $j = k > i$ and fix $z_k = zp^{\alpha-k+1}$ in K_k. Since $j = k$, the computation (A.3) tells us that for each x_i in K_i, there exists a unique $y_j = z - xp^{j-i}$ such that $x_i + y_j = z_k$. Thus, $a_{i,j,k} = |K_i| = \phi(p^{i-1})$.

The proof of (c) is somewhat more involved. Let $i = j = k$ and fix $z_k = zp^{\alpha-k+1}$ where $p \nmid z$. For any element $x_i = xp^{n-k+1}$ of $K_i = K_k$, there exists a unique a_0 in $\mathbb{Z}/p^\alpha\mathbb{Z}$ such that

$$x_i + a_0 = z_k. \tag{A.4}$$

Since $p^{\alpha-k+1}$ divides both x_i and z_k, it must also divide a_0, so that we can write $a_0 = ap^{n-k+1}$ for some a. In light of (A.4), we now have $x + a = z$, so that $a = z - x$.

Therefore a_0 belongs to K_k if and only if $p \nmid (z-x)$. We now note that if $p|(z-x)$, then x_i would serve as a solution to $x_i + y = z_k$ where y belongs to some K_ℓ with $\ell < i = k$. By statement (b), it follows that

$$\begin{aligned} a_{i,j,k} &= |K_k| - \sum_{\ell=1}^{k-1} \phi\bigl(p^{\ell-1}\bigr) \\ &= \phi\bigl(p^k\bigr) - \sum_{\ell=2}^{k-1}\bigl(p^{\ell-1} - p^{\ell-2}\bigr) - 1 \\ &= \bigl(p^{k-1} - p^{k-2}\bigr) - \bigl(p^{k-2} - p^{k-3}\bigr) - \cdots - (p-1) - 1 \\ &= p^{k-1} - 2p^{k-2}, \end{aligned}$$

as claimed.

Now we consider statement (d). Suppose that $j > k$ and $i \neq j$. In light of (A.1), we may assume that $i < j$. Maintaining the same notation and conventions as in the proof of statement (a), we again arrive at (A.3) and conclude that $x_i + y_j$ belongs to K_j. Since $j > k$, we conclude that $a_{i,j,k} = 0$.

Finally, let us prove (e). Suppose that $i = j > k$ and let $z_k = zp^{\alpha-k+1}$ in K_k be given. For each $x_i = xp^{\alpha-i+1}$ in K_i, we have

$$xp^{\alpha-i+1} + \bigl(zp^{i-k} - x\bigr)p^{\alpha-i+1} = \bigl(zp^{i-k}\bigr)p^{\alpha-i+1} = zp^{\alpha-k+1} = z_k. \tag{A.5}$$

Now $p|(zp^{i-k})$ because $i > k$, so it follows that $p \nmid (zp^{i-k} - x)$ since $p \nmid x$. Therefore $(zp^{i-k} - x)p^{\alpha-i+1}$ belongs to K_i. Looking at (A.5), we conclude that for each x_i in K_i, there exists a unique y_i in K_i such that $x_i + y_i = z_k$. Since $i = j$, we conclude that $a_{i,j,k} = |K_i| = \phi(p^{i-1})$, as desired. □

Having proven the preceding lemma, it is now straightforward to see that M_i has the form (4.11). The complete reasoning is presented below.

(1) If $j, k < i$, then $(M_i)_{j,k} = 0$. In other words, the upper-left $(i-1) \times (i-1)$ submatrix of M_i contains only zeros. Indeed, letting $i' = j$ and $j' = i > k$ (so that $i' \neq j'$ since $j < i$), it follows that $(M_i)_{j,k} = a_{i,j,k} = a_{j,i,k} = a_{i',j',k} = 0$ by (A.1) and (d) of Lemma A.1.
(2) If $j < i = k$, then $(M_i)_{j,k} = \phi(p^{j-1})$, so that the first $i-1$ entries of the ith column of M_i are given by $1, \phi(p), \phi(p^2), \ldots, \phi(p^{i-2})$. As before, we set $i' = j$ and $j' = i$ and observe that $(M_i)_{j,k} = a_{i,j,k} = a_{j,i,k} = a_{i',j',k} = \phi(p^{i'-1}) = \phi(p^{j-1})$ by (b) of Lemma A.1 since $j' = k > i'$.
(3) If $i = j > k$, then $(M_i)_{j,k} = \phi(p^{i-1})$, so that the first $(i-1)$ entries of the ith row of M_i are each $\phi(p^{i-1})$. To see this, simply note that $(M_i)_{j,k} = a_{i,j,k} = \phi(p^{i-1})$ by (e) of Lemma A.1.
(4) If $i = j = k$, then $(M_i)_{j,k} = a_{i,i,i} = p^{i-1} - 2p^{i-2}$ by (c) of Lemma A.1.
(5) If $j = k > i$, then $(M_i)_{j,k} = \phi(p^{i-1})$. In other words, the final $(n+1-i)$ entries along the main diagonal of M_i are $\phi(p^{i-1})$. This follows immediately from (b) of Lemma A.1.

(6) If $j > i, k$, then $(M_i)_{j,k} = 0$ follows from (d) of Lemma A.1. Therefore the final $(n + 1 - i)$ rows of M_i have only zeros to the left of the main diagonal.
(7) If $i, j < k$, then $(M_i)_{j,k} = 0$. In other words, the last $(n + 1 - i)$ columns of M_i have only zeros above the main diagonal. This follows immediately from (a) of Lemma A.1.

References

1. Aguiar, M., Andre, C., Benedetti, C., Bergeron, N., Chen, Z., Diaconis, P., Hendrickson, A., Hsiao, S., Isaacs, I.M., Jedwab, A., Johnson, K., Karaali, G., Lauve, A., Le, T., Lewis, S., Li, H., Magaard, K., Marberg, E., Novelli, J.-C., Pang, A., Saliola, F., Tevlin, L., Thibon, J.-Y., Thiem, N., Venkateswaran, V., Ryan Vinroot, C., Yan, N., Zabrocki, M.: Supercharacters, symmetric functions in noncommuting variables, and related Hopf algebras. Adv. Math. **229**, 2310–2337 (2012)
2. Anderson, D.R., Apostol, T.M.: The evaluation of Ramanujan's sum and generalizations. Duke Math. J. **20**, 211–216 (1953)
3. André, C.A.M.: Basic characters of the unitriangular group. J. Algebra **175**(1), 287–319 (1995)
4. André, C.A.M.: The basic character table of the unitriangular group. J. Algebra **241**(1), 437–471 (2001)
5. André, C.A.M.: Basic characters of the unitriangular group (for arbitrary primes). Proc. Am. Math. Soc. **130**(7), 1943–1954 (2002). (Electronic)
6. André, C.A.M., Neto, A.M.: A supercharacter theory for the Sylow p-subgroups of the finite symplectic and orthogonal groups. J. Algebra **322**, 1273–1294 (2009)
7. Arias-Castro, E., Diaconis, P., Stanley, R.: A super-class walk on upper-triangular matrices. J. Algebra **278**(2), 739–765 (2004)
8. Balandraud, É.: An application of Ramanujan sums to equirepartition modulo an odd integer. Unif. Distrib. Theory **2**(2), 1–17 (2007)
9. Benidt, S.G., Hall, W.R.S., Hendrickson, A.O.F.: Upper and lower semimodularity of the supercharacter theory lattices of cyclic groups. arXiv:1203.1638
10. Brumbaugh, J.L., Bulkow, M., Fleming, P.S., Garcia, L.A., Garcia, S.R., Karaali, G., Michal, M., Turner, A.P.:. Supercharacters, exponential sums, and the uncertainty principle. Preprint. http://arxiv.org/abs/1208.5271
11. Cohen, E.: An extension of Ramanujan's sum. Duke Math. J. **16**, 85–90 (1949)
12. Cohen, E.: Trigonometric sums in elementary number theory. Am. Math. Mon. **66**, 105–117 (1959)
13. Curtis, C.W., Reiner, I.: Representation Theory of Finite Groups and Associative Algebras. Pure and Applied Mathematics, vol. XI. Interscience, New York (1962)
14. Diaconis, P., Isaacs, I.M.: Supercharacters and superclasses for algebra groups. Trans. Am. Math. Soc. **360**(5), 2359–2392 (2008)
15. Diaconis, P., Thiem, N.: Supercharacter formulas for pattern groups. Trans. Am. Math. Soc. **361**(7), 3501–3533 (2009)
16. Droll, A.: A classification of Ramanujan unitary Cayley graphs. Electron. J. Comb. **17**(1), 6 (2010). Note 29
17. Erdős, P., Vaughan, R.C.: Bounds for the r-th coefficients of cyclotomic polynomials. J. Lond. Math. Soc. **8**, 393–400 (1974)
18. Fleming, P.S., Garcia, S.R., Karaali, G.: Classical Kloosterman sums: representation theory, magic squares, and Ramanujan multigraphs. J. Number Theory **131**(4), 661–680 (2011)
19. Hardy, G.H.: Ramanujan. Twelve Lectures on Subjects Suggested by His Life and Work. Cambridge University Press, Cambridge (1940)
20. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, 5th edn. Clarendon, New York (1979)
21. Haukkanen, P.: Regular class division of integers (mod r). Notes Number Theory Discret. Math. **6**(3), 82–87 (2000)
22. Hendrickson, A.O.F.: Supercharacter theories of cyclic p-groups. ProQuest LLC, Ann Arbor, MI, 2008. Thesis (Ph.D.). The University of Wisconsin, Madison. (2008)
23. Hendrickson, A.O.F.: Supercharacter theory constructions corresponding to Schur ring products. Commun. Algebra **40**(12), 4420–4438 (2012). doi:10.1080/00927872.2011.602999

24. Hölder, O.: Fusions of character tables and Schur rings of abelian groups. Pr. Mat.-Fiz. **43**, 13–23 (1936)
25. Humphries, S.P., Johnson, K.W.: Fusions of character tables and Schur rings of abelian groups. Commun. Algebra **36**(4), 1437–1460 (2008)
26. Isaacs, I.M.: Character Theory of Finite Groups. AMS Chelsea Publishing, Providence (2006). Corrected reprint of the 1976 original. Academic Press, New York, MR0460423
27. James, G., Liebeck, M.: Representations and Characters of Groups, 2nd edn. Cambridge University Press, New York (2001)
28. Jensen, J.L.W.V.: Et nyt udtryk for den talteoretiske funktion $\sigma\mu(n) = m(n)$. In: Beretning on dem 3 Skandinaviske Matematiker-Kongres (1915)
29. Johnson, K.W., Smith, J.D.H.: Characters of finite quasigroups. III. Quotients and fusion. Eur. J. Comb. **10**(1), 47–56 (1989)
30. Johnson, K.R.: A reciprocity law for Ramanujan sums. Pac. J. Math. **98**(1), 99–105 (1982)
31. Johnson, K.R.: Reciprocity in Ramanujan's sum. Math. Mag. **59**(4), 216–222 (1986)
32. Johnson, K.W., Poimenidou, E.: Generalised classes in groups and association schemes: Duals of results on characters and sharpness. Eur. J. Comb. **20**(1), 87–92 (1999)
33. Jutila, M.: Distribution of rational numbers in short intervals. Ramanujan J. **14**(2), 321–327 (2007)
34. Kesava Menon, P.: On Vaidyanathaswamy's class division of the residue classes modulo 'N'. J. Indian Math. Soc. **26**, 167–186 (1962)
35. Kesava Menon, P.: On functions associated with Vaidyanathaswamy's algebra of classes mod n. Indian J. Pure Appl. Math. **3**(1), 118–141 (1972)
36. Kluyver, J.C.: Some formulae concerning the integers less than n and prime to n. In: Proceedings of the Royal Netherlands Academy of Arts and Sciences (KNAW), vol. 9, pp. 408–414 (1906)
37. Konvalina, J.: A generalization of Waring's formula. J. Comb. Theory, Ser. A **75**(2), 281–294 (1996)
38. Kutzko, P.C.: The cyclotomy of finite commutative P.I.R.'s. Ill. J. Math. **19**, 1–17 (1975)
39. Landau, E.: Handbuch der Lehre von der Verteilung der Primzahlen, vol. 2, 2nd edn. Chelsea, New York (1953). With an appendix by P.T. Bateman
40. Lehmer, D.H.: Mahler's matrices. J. Aust. Math. Soc. **1**, 385–395 (1959/1960)
41. Lucht, L.G.: A survey of Ramanujan expansions. Int. J. Number Theory **6**(8), 1785–1799 (2010)
42. Maze, G.: Partitions modulo n and circulant matrices. Discrete Math. **287**(1–3), 77–84 (2004)
43. McCarthy, P.J.: Introduction to Arithmetical Functions. Universitext. Springer, New York (1986)
44. Motose, K.: Ramanujan's sums and cyclotomic polynomials. Math. J. Okayama Univ. **47**, 65–74 (2005)
45. Nanda, V.C.: Generalizations of Ramanujan's sum to matrices. J. Indian Math. Soc. **48**(1–4), 177–187 (1986). 1984
46. Nathanson, M.B.: Additive Number Theory. Graduate Texts in Mathematics, vol. 164. Springer, New York (1996). The classical bases
47. Nicol, C.A.: Some formulas involving Ramanujan sums. Can. J. Math. **14**, 284–286 (1962)
48. Planat, M., Minarovjech, M., Saniga, M.: Ramanujan sums analysis of long-period sequences and $1/f$ noise. Europhys. Lett. **85**, 40005 (2009)
49. Planat, M., Rosu, H., Perrine, S.: Ramanujan sums for signal processing of low-frequency noise. Phys. Rev. A **66**(5), 056128 (2002)
50. Planat, M., Rosu, H.C.: Cyclotomy and Ramanujan sums in quantum phase locking. Phys. Lett. A **315**(1–2), 1–5 (2003)
51. Ramanathan, K.G.: Some applications of Ramanujan's trigonometrical sum $C_m(n)$. Proc. Indian Acad. Sci., Sect. A **20**, 62–69 (1944)
52. Ramanathan, K.G., Subbarao, M.V.: Some generalizations of Ramanujan's sum. Can. J. Math. **32**(5), 1250–1260 (1980)
53. Ramanujan, S.: On certain trigonometrical sums and their applications in the theory of numbers. In: Collected papers of Srinivasa Ramanujan, pp. 179–199. AMS Chelsea Publ., Providence (2000). Trans. Cambridge Philos. Soc. **22**(13), 259–276 (1918)
54. Ramaré, O.: Eigenvalues in the large sieve inequality. Funct. Approx. Comment. Math. **37**(part 2), 399–427 (2007)
55. Rao, K.N., Sivaramakrishnan, R.: Ramanujan's sum and its applications to some combinatorial problems. In: Proceedings of the Tenth Manitoba Conference on Numerical Mathematics and Computing, Vol. II, Winnipeg, Man., 1980, vol. 31, pp. 205–239 (1981)
56. Schwarz, W.: Ramanujan expansions of arithmetical functions. In: Ramanujan revisited, Urbana-Champaign, Ill., 1987, pp. 187–214. Academic Press, Boston (1988)

57. Schwarz, W., Spilker, J.: An introduction to elementary and analytic properties of arithmetic functions and to some of their almost-periodic properties In: Arithmetical Functions. London Mathematical Society Lecture Note Series, vol. 184. Cambridge University Press, Cambridge (1994)
58. Sugunamma, M.: Eckford Cohen's generalizations of Ramanujan's trigonometrical sum $C(n, r)$. Duke Math. J. **27**, 323–330 (1960)
59. Tam, T.-Y.: On the cyclic symmetry classes. J. Algebra **182**(3), 557–560 (1996)
60. Thiem, N.: Branching rules in the ring of superclass functions of unipotent upper-triangular matrices. J. Algebr. Comb. **31**(2), 267–298 (2010)
61. Thiem, N., Venkateswaran, V.: Restricting supercharacters of the finite group of unipotent uppertriangular matrices. Electron. J. Comb. **16**(1), 32 (2009). Research paper 23
62. Tóth, L.: Some remarks on Ramanujan sums and cyclotomic polynomials. Bull. Math. Soc. Sci. Math. Roum. **53**(101), 277–292 (2010)
63. von Sterneck, R.D.: Sitzungsber. Math.-Natur. Kl. Kaiserl. Akad. Wiss. Wien **111**, 1567–1601 (1902)
64. Yan, N.: Representation Theory of the Finite Unipotent Linear Groups. Ph.D. thesis, University of Pennsylvania (2001). Also see [65]
65. Yan, N.: Representations of finite unipotent linear groups by the method of clusters. ArXiv e-prints, April 2010