GRAPHICAL CYCLIC SUPERCHARACTERS FOR COMPOSITE MODULI

BOB LUTZ

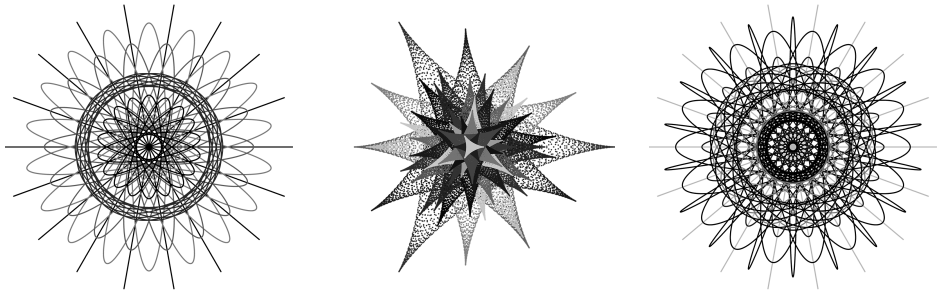
Abstract. Recent work has introduced the study of graphical properties of cyclic supercharacters, functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ whose values are exponential sums with close connections to Gauss sums and Gaussian periods. Plots of these functions exhibit striking features, some of which have been previously explained when the modulus n is a power of an odd prime. After reviewing this material, we initiate the graphical study of images of cyclic supercharacters in the case of composite n.

1. Introduction

For a positive integer n and a unit ω mod n of order d, the associated *cyclic supercharacter mod* n is the function $\sigma_\omega : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ given by

$$\sigma_\omega(y) = \sum_{j=1}^{d} e\left(\frac{\omega^j y}{n}\right),$$

where $e(\theta) := \exp(2\pi i\theta)$ for all real θ. Gauss studied the values of cyclic supercharacters mod primes $p > 2$, called *Gaussian periods*, as they relate to the problem of drawing regular polygons with compass and straight-edge. These values are modernly called *Gaussian periods* and have appeared in many contexts, including the construction of difference sets and the optimized AKS algorithm of Lenstra and Pomerance [1, 15]. A more detailed account of the history of Gaussian periods with references can be found in [13], although our notation differs from theirs.



(A) $n = 478125$, $\omega = 3124$ (B) $n = 551905$, $\omega = 20719$ (C) $n = 455175$, $\omega = 107218$

Figure 1. Realized as complex plots, the images of cyclic supercharacters σ_ω mod n reveal themselves in surprising ways.

2010 *Mathematics Subject Classification.* Primary 11L03; Secondary 11L05, 11T24.

Kummer introduced analogous sums, values of cyclic supercharacters $\sigma_\omega \bmod n$, for composite n. These sums have been studied in their own right and linked to certain difference sets [8, 9, 14]. While individual values can be difficult to analyze, recent work has revealed striking and accessible patterns in these sums when viewed together as the image $\mathrm{im}(\sigma_\omega)$ of a cyclic supercharacter for a fixed modulus n and generator ω. Figure 1 offers a small gallery of such images as complex plots.

For n a power of an odd prime, much of this graphical behavior has been described previously in terms of certain Laurent polynomials on high-dimensional tori [7, 13]. We review this material briefly in Section 2. Comparatively little, however, has been done to study the analogous properties of cyclic supercharacters mod non-prime-power n. With this note, we aim to explain concisely and systematically many of the patterns yet observed in the images of these supercharacters.

For convenience, we will frequently consider cyclic supercharacters σ_ω as periodic functions on $\mathbb{Z}$ with period n, and treat integers tacitly as residues whenever it does not affect the statement. The functions σ_ω are supercharacters in the sense of [6], but we do not adopt this perspective here. Ramanujan sums, Heilbronn sums, and generalized Kloosterman sums can also be viewed as values of supercharacters [3, 4, 12]. For cyclic supercharacters, the motivated reader can find the details of this approach in [7].

2. Prime-power moduli

In this section, we consider cyclic supercharacters mod p^a for an odd prime p and positive integer a. There is a description, due to [7], of the images of such supercharacters in terms of the images of certain Laurent polynomials, which we record below. Throughout, we write φ for the totient function, $\mathbb{T}$ for the unit circle in $\mathbb{C}$, and $\Phi_d(x)$ for the dth cyclotomic polynomial in x. Recall that $\Phi_d(x)$ is monic and has all integer coefficients.

Theorem 2.1. *Fix a positive integer d. If $p \equiv 1 \pmod d$ is an odd prime and ω is a unit of order d mod p^a for some positive integer a, then $\operatorname{im}\sigma_\omega$ is contained in the image of the function $g_d : \mathbb{T}^{\varphi(d)} \to \mathbb{C}$ given by*

$$g_d(z_1, \ldots, z_{\varphi(d)}) = \sum_{k=1}^{d} \prod_{j=1}^{\varphi(d)} z_j^{c_{j,k}},$$

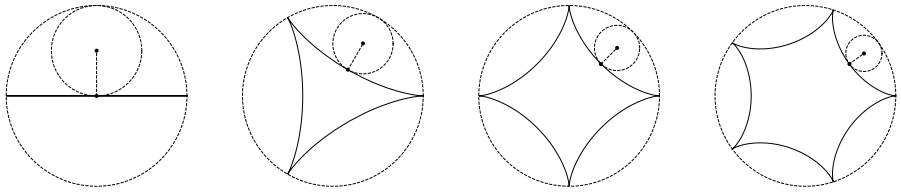
where the exponents $c_{j,k}$ are integers determined by the relations

$$x^k \equiv \sum_{j=1}^{\varphi(d)} c_{j,k} x^{j-1} \pmod{\Phi_d(x)}.$$

Moreover, every open disk in the image of g_d contains points in the images of σ_ω for sufficiently large p^a subject to $p \equiv 1 \pmod d$.

For $k = 1, 2, \ldots$ let $A_k \subset \mathbb{C}$. If there exists a set $B \subset \mathbb{C}$ such that $A_k \subset B$ for all k and, for each nonempty open set $U \subset B$, a positive integer k_U for which $k > k_U$ implies that $U \cap A_{k_U}$ is nonempty, then we say that the sets A_k *fill out* B as $k \to \infty$. In these terms, we can rephrase the last statement of Theorem 2.1 by saying that the images $\mathrm{im}(\sigma_\omega)$ fill out $\operatorname{im} g_d$ as $p^a \to \infty$ subject to $p \equiv 1 \pmod d$.

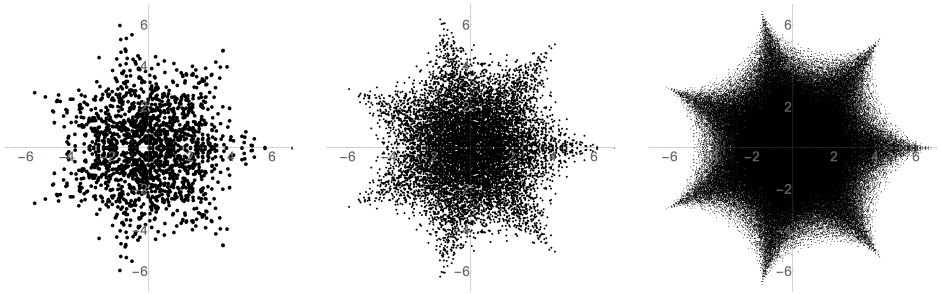
The clearest behavior occurs when, in the notation of Theorem 2.1, d is a positive power of an odd prime. Recall that a *hypocycloid* is a planar curve obtained by



(A) Tusi couple (B) Deltoid (C) Astroid (D) 5-hypocycloid

FIGURE 2. A circle of radius 1 traces out hypocycloids as it rolls within circles of radii 2, 3, 4, and 5.

tracing a fixed point on a circle as it rolls within a larger circle. This construction, illustrated in Figure 2, produces a simple closed curve if the smaller radius divides the larger; the number of cusps is the ratio of the larger radius to the smaller. For all integers $k \geq 2$, let $H_k \subset \mathbb{C}$ denote the compact, simply-connected set whose boundary is the k-cusped hypocycloid centered at 0 with a cusp at k. Let P_k denote the convex hull of H_k, whose boundary is the regular k-gon centered at 0 with a vertex at k.



(A) $(113^2, 129)$ (B) $(43^3, 3623)$ (C) $(1289^2, 341010)$

FIGURE 3. For the given pairs (n, ω), the images of the cyclic supercharacters σ_ω mod n are on their way to filling out H_7.

If ℓ is an odd prime, then $\varphi(\ell) = \ell - 1$ and $\Phi_\ell(x) = 1 + x + x^2 + \cdots + x^{\ell-1}$, so

$$g_\ell(z_1, \ldots, z_{\ell-1}) = z_1 + z_2 + \cdots + z_{\ell-1} + \frac{1}{z_1 z_2 \cdots z_{\ell-1}}.$$

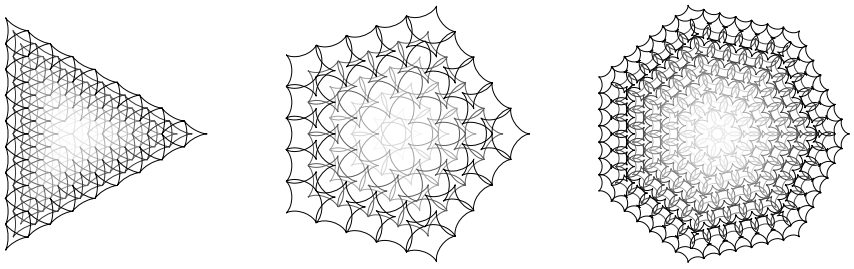
The image of g_ℓ is seen to be $\mathrm{Tr}(\mathrm{SU}_\ell(\mathbb{C}))$, which is precisely H_ℓ [5, Theorem 3.2.3]. More is true, but we require additional notation to write it succinctly. In Figure 3, several terms of a sequence filling out H_7 are illustrated.

For nonempty subsets A and B of $\mathbb{C}$, make the definitions

$$\begin{aligned} A \oplus B &= \{a + b : (a, b) \in A \times B\} \\ A \otimes B &= \{ab : (a, b) \in A \times B\}. \end{aligned} \tag{1}$$

The sets in (1) are sometimes called the *Minkowski sum* and *Minkowski product*, respectively, of A and B, and the operations $\oplus$ and $\otimes$ are called *Minkowski addition* and *Minkowski multiplication*. The corresponding n-ary operations are defined by induction; for convenience, we write $A \oplus \cdots \oplus A$ as $A^{\oplus k}$, where k is the number of

summands. While Minkowski addition and multiplication are both commutative and have identity elements, neither distributes over the other or has a well-defined inverse operation. Minkowski addition has been studied extensively over $\mathbb{R}^n$ and is well understood, at least compared to Minkowski multiplication, which is an active subject of research in pure and applied settings [10, 11, 16].



(A) $\ell = b = 3$ (B) $\ell = 5$, $b = 2$ (C) $\ell = 7$, $b = 2$

FIGURE 4. The outer boundaries in the figures form the boundaries of the Minkowski sums $H_\ell^{\oplus \ell^{b-1}}$.

For the moment, we are concerned with Minkowski addition. If ℓ^b is a positive power of an odd prime ℓ, then it can be shown that

$$\operatorname{im}(g_{\ell^b}) = H_\ell^{\oplus \ell^{b-1}}. \tag{2}$$

Several of these sets are illustrated in Figure 4. The reader might notice that as ℓ^b increases, the figures begin to resemble regular polygons. Indeed, it follows from a corollary to the Shapley–Folkman theorem in [17] that as $k \to \infty$, the scaled Minkowski sums $\frac{1}{k} H_\ell^{\oplus k}$ fill out P_ℓ. To close the section, we record the corresponding implication for cyclic supercharacters. The proof is an application of the preceding discussion to Theorem 2.1.

Proposition 2.2. *Fix an odd prime ℓ. For $k = 1, 2, \ldots$ let b_k be a positive integer, $p_k > \ell$ an odd prime with $\ell^{b_k} | \varphi(p_k^{a_k})$, and ω_k a unit mod $p_k^{a_k}$ of order ℓ^{b_k}. As $k \to \infty$, if $b_k \to \infty$, then the scaled images $\ell^{1-b_k} \operatorname{im}(\sigma_{\omega_k})$ fill out P_ℓ.*

3. Composite moduli

We turn our attention now to cyclic supercharacters whose moduli are not a power of a prime. Let a and b be integers. For a unit ω mod a, we denote by $\operatorname{ord}(\omega)$ the (multiplicative) order of ω. Unless indicated otherwise, (a, b) will denote the GCD of a and b. If $b|a$, then unless necessary, we will not distinguish between ω and its image under the reduction map $\mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$. When we wish to emphasize the change in modulus, we shall write the residue of ω mod b as ω_b.

3.1. **General behavior.** We recall some elementary geometric notions. A set $A \subset \mathbb{C}$ is said to have *k-fold dihedral symmetry* if it is invariant under the action on $\mathbb{C}$ of the dihedral group of order $2k$ by complex conjugation and rotation by $2\pi/k$ about the origin. The intersection of all supersets of A having k-fold dihedral symmetry is called the *k-fold dihedral closure* of A. Equivalently, this is the union

of the orbits of all points in A. If A is closed under complex conjugation, then its k-fold dihedral closure is

$$\{e(j/k) : j = 1, \ldots, k\} \otimes A. \tag{3}$$

Proposition 3.1(a) below is an extension of [7, Proposition 3.1]. Proposition 3.1(b) is a useful observation in the vein of Section 2.

Proposition 3.1. *Let σ_ω be a cyclic supercharacter mod n, and write $k = (\omega - 1, n)$.*

(a) The k-fold dihedral closure of $\mathrm{im}(\sigma_{\omega_{n/k}})$ is $\mathrm{im}(\sigma_\omega)$.

(b) If $k = 1$ and $\mathrm{ord}(\omega) > 1$, then $\mathrm{im}(\sigma_\omega) \subset H_{\mathrm{ord}(\omega)}$.

Proof. Since $k = (\omega - 1, n)$, we have $\mathrm{ord}(\omega_{n/k}) = \mathrm{ord}(\omega)$. For $j = 1, \ldots, \mathrm{ord}(\omega)$, write $\omega^j = 1 + r_j k$ and notice that

$$\sigma_\omega\left(y + n/k\right) = \sum_{j=1}^{\mathrm{ord}(\omega)} e\left(\frac{(1 + r_j k)(y + n/k)}{n}\right) = e(1/k)\sigma_{\omega_{n/k}}(y),$$

since $\mathrm{ord}(\omega) = \mathrm{ord}(\omega_{n/k})$. Combine this with the fact that $\sigma_\omega(-y) = \overline{\sigma_\omega(y)}$ to obtain Proposition 3.1(a). For 3.1(b), notice that $\omega + \omega^2 + \cdots + \omega^{\mathrm{ord}(\omega)} = 0$, so

$$\sigma_\omega(y) = e\left(\frac{-(\omega + \cdots + \omega^{\mathrm{ord}(\omega)-1})y}{n}\right) + \sum_{j=1}^{\mathrm{ord}(\omega)-1} e\left(\frac{\omega^j y}{n}\right).$$

In particular, $\mathrm{im}(\sigma_\omega) \subset \mathrm{Tr}(\mathrm{SU}_{\mathrm{ord}(\omega)}(\mathbb{C}))$. Appealing to [5, Theorem 3.2.3] completes the proof. □

3.2. **A new perspective.** Many patterns recognizable in the plots of cyclic supercharacters can be explained by the following overlooked mechanism. The remainder of the article is dedicated to consequences of Theorem 3.2.

Theorem 3.2. *Suppose that σ_ω is a cyclic supercharacter mod mn for positive integers m and n. If $\mathrm{ord}(\omega_n) = uv$ where $(v, \mathrm{ord}(\omega_m)) = 1$, then*

$$\sigma_\omega(sm + tn) = \sum_{j=1}^{u} \sigma_{\omega_m^u}(\omega^j t)\sigma_{\omega_n^u}(\omega^j s),$$

for all integers of the form $sm + tn$.

Proof. Let d be the order of ω. We have

$$\begin{aligned}
\sigma_\omega(sm + tn) &= \sum_{j=1}^{d} e\left(\frac{\omega^j(sm + tn)}{mn}\right) \\
&= \sum_{j=1}^{uv} \sum_{k=1}^{d/(uv)} e\left(\frac{\omega^{j+uvk} s}{n}\right) e\left(\frac{\omega^{j+uvk} t}{m}\right) \\
&= \sum_{j=1}^{uv} e\left(\frac{\omega^j s}{n}\right) \sum_{k=1}^{d/(uv)} e\left(\frac{\omega^j \omega^{uvk} t}{m}\right) \\
&= \sum_{j=1}^{uv} e\left(\frac{\omega^j s}{n}\right) \sigma_{\omega_m^{uv}}(\omega^j t).
\end{aligned}$$

Since $(v, \operatorname{ord}(\omega_m)) = 1$, we have $\omega_m^{uv} = \omega_m^u$. Moreover, it is not difficult to show that $\sigma_{\omega_m^u}(\omega^j t)$ depends only on the residue of of j mod u. Hence

$$\sigma_\omega(sm + tn) = \sum_{j=1}^{u} \sigma_{\omega_m^u}(\omega^j t) \sum_{k=1}^{v} e\left(\frac{\omega^{j+ku} s}{n}\right) = \sum_{j=1}^{u} \sigma_{\omega_m^u}(\omega^j t)\sigma_{\omega_n^u}(\omega^j s). \qquad \square$$

Corollary. *If $u = 1$ in the above notation, so $(\operatorname{ord}(\omega_m), \operatorname{ord}(\omega_n)) = 1$, then*

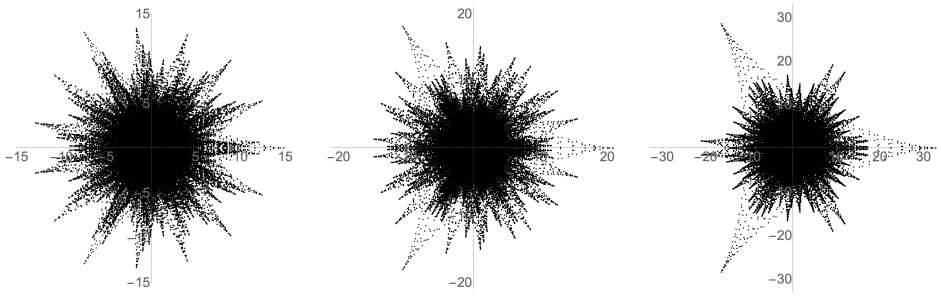
$$\sigma_\omega(sm + tn) = \sigma_{\omega_m}(t)\sigma_{\omega_n}(s).$$

In particular, $\operatorname{im}(\sigma_\omega) = \operatorname{im}(\sigma_{\omega_m}) \otimes \operatorname{im}(\sigma_{\omega_n})$.

Induction on the corollary yields [7, Theorem 2.1], although the statement there lacks a necessary hypothesis. Applying this fact to the discussion in Section 2 gives the following result, which connects images of cyclic supercharacters with Minkowski products of hypocycloids and regular polygons.

Proposition 3.3. *Fix a positive integer k and distinct odd primes $\ell_1, \ldots, \ell_k$. For each $j = 1, \ldots, k$, let A_j be either P_{ℓ_j} or $H_{\ell_j}^{\oplus b_j}$ for some positive integer b_j. There is a sequence of cyclic supercharacters whose images, when scaled appropriately, fill out $A_1 \otimes \cdots \otimes A_k$. Moreover, scaling is only necessary if $A_j = P_{\ell_j}$ for some j.*

In Figure 5 we plot individual terms of sequences described in Proposition 3.3, where $k = 2$ and $A_1 = H_3$. While the boundary of the Minkowski product $H_{\ell_1} \otimes H_{\ell_2}$ ought to have $\ell_1\ell_2$ cusps, each of the plots in Figures 5(B) and 5(C) exhibits only 3. This is because the values of σ_{ω_n} are concentrated toward the origin and hence far from the non-real cusps of H_{ℓ_2}. In order for the image of σ_ω to resemble $H_3 \otimes H_{\ell_2}$, larger values of n are necessary. In Figure 5(A), the expected 15 cusps are more evident.



(A) $(1033, 1031, 219191)$ (B) $(1153, 1163, 120562)$ (C) $(1399, 1409, 240237)$

FIGURE 5. For the given triples (m, n, ω), the values of the cyclic supercharacters σ_ω mod mn belong to $H_3 \otimes H_{\ell_2}$ where, from left to right, $r_2 = 5$, 7 and 11.

There is no obvious characterization of $H_a \otimes H_b$, such as a parametrization of its boundary, even in terms of parametrizations of the boundaries of H_a and H_b. We can, however, give a concrete description of the boundary of the Minkowski product of two polygons that does not appear to have been recorded previously. We defer the proof, an application of [16, Theorem 2.4], to the Appendix.

Proposition 3.4. *For odd primes $k < \ell$, the boundary of $P_k \otimes P_\ell$ is contained in the $k\ell$-fold dihedral closure of the union of line segments connecting $k\ell e(\frac{1}{k} - \frac{1}{\ell})$ to $k\ell e(\frac{1}{k} + \frac{1}{\ell})$ and $k\ell \cos(\frac{\pi}{k})/\cos(\frac{\pi}{\ell})$.*

3.3. **Gauss sums.** Henceforth, p will denote an odd prime number. Recall that a *character* mod p is a group map $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{T}$. For each integer k, let χ^k be the character $x \mapsto \chi(x)^k$, and recall that the *order* of χ is the smallest positive k for which χ^k is identically 1. For each p, the unique character mod p of order 2 is the familiar Legendre symbol.

There are two types of exponential sum bearing the name *Gauss sum mod p of order k*, which we distinguish by their notation. The first, defined for any positive divisor k of $\varphi(p)$, is the function $g_k : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}$ given by

$$g_k(t) = \sum_{j=1}^{p} e\left(\frac{tj^k}{p}\right).$$

This object differs from the functions g_d appearing in Theorem 2.1; the conflict of notation is an unfortunate coincidence. From now on, we will use g_k to refer to Gauss sums. For all t coprime to p, notice that

$$g_1(t) = \sum_{j=0}^{p-1} e(t/p)^j = \frac{1 - e(t/p)^p}{1 - e(t/p)} = 0. \tag{4}$$

The second type of *Gauss sum mod p of order k*, defined in terms of a character χ mod p of order k, is also a function $G(\cdot, \chi) : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}$, this time given by

$$G(t, \chi) = \sum_{j=1}^{p-1} \chi(j) e\left(\frac{tj}{p}\right).$$

We write $G(\chi) = G(1, \chi)$ and make tacit use of the following identities:

$$G(t, \chi) = \overline{\chi(t)} G(\chi) = \chi(-1)\overline{G(t, \overline{\chi})}.$$

The two types of Gauss sum are related by

$$g_k(t) = \sum_{j=1}^{k-1} G(t, \chi^j). \tag{5}$$

In addition to proofs of the last few facts, the reader can find in [2] explicit evaluations of g_k for small k up to certain sign ambiguities, some of which persist to this day. Gauss resolved the issue for g_2 in terms of the Legendre symbol χ by showing that

$$\chi(t) g_2(t) = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \pmod 4 \\ i\sqrt{p}, & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{6}$$

The next two lemmas are of technical import only; the casual reader is invited to skim their proofs, although they are used in what follows. We denote the real part of a complex number z by $\Re(z)$ and the imaginary part by $\Im(z)$.

Lemma 3.5. *If, in addition to the hypotheses of Theorem 3.2, $m = p$ is an odd prime, ω_p is a primitive root mod p, and t a unit mod p, then*

$$\sigma_\omega(sm + tn) = \frac{1}{(u, \varphi(p))} \sum_{j=1}^{u} (g_{(u,\varphi(p))}(\omega^j t) - 1) \sigma_{\omega_n^u}(\omega^j s). \tag{7}$$

Proof. To Theorem 3.2, apply the observation that

$$g_k(r) - 1 = k \sum_{j=1}^{\varphi(p)/k} e\left(\frac{r\omega^{jk}}{p}\right) = k\sigma_{\omega^k}(r). \qquad \square$$

Lemma 3.6. *If k is a positive even integer and $p \equiv 1 \pmod{2k}$ is an odd prime, then g_k is real valued.*

Proof. Let χ be a character mod p of order k. We have

$$\begin{aligned} g_k(t) &= \sum_{j=1}^{k-1} G(t, \chi^j) \\ &= G(t, \chi^{k/2}) + \sum_{j=1}^{k/2-1} G(t, \chi^j) + \sum_{j=1}^{k/2-1} G(t, \overline{\chi}^j) \\ &= g_2(t) + \sum_{j=1}^{k/2-1} G(t, \chi^j) + \sum_{j=1}^{k/2-1} \chi^j(-1) G(t, \overline{\chi}^j) \\ &= g_2(t) + \sum_{j=1}^{k/2-1} G(t, \chi^j) + \sum_{j=1}^{k/2-1} (-1)^{j\varphi(p)/u} G(t, \overline{\chi}^j) \\ &= g_2(t) + 2 \sum_{j=1}^{k/2-1} \Re(G(t, \chi^j)), \end{aligned}$$

where $g_2(t)$ is real by (6). $\square$

3.4. **Main results.** For the rest of the article, it will suit us to treat $\mathbb{C}$ as an $\mathbb{R}$-algebra with basis $(1, i)$, so that if $z = \alpha + i\beta$ for real α and β, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{pmatrix} = (a\alpha + b\beta) + i(c\alpha + d\beta).$$

The following results are typical consequences of Lemma 3.5. By exploiting the additional requirement that ω_n be a root of -1, we are able to write σ_ω in terms of $\sigma_{\omega_n^u}$ subject to certain $\mathbb{R}$-linear transformations. When the corresponding matrix representations have at most 2 nonzero entries, we obtain explanations of various graphical features, including some depicted in [7] and [12], which is our goal. Ellipses, rhombi, astroids, and other plane figures lurk in the images of the cyclic supercharacters described by Theorem 3.7. We present several examples in the next section.

Theorem 3.7. *In the notation of Theorem 3.2, suppose that u is even, v odd, and $m = p$ an odd prime. Let r be a positive integer, and suppose further that $\omega_n^{uv/2} = -1$, $\operatorname{ord}(\omega_p) = \frac{1}{r}\varphi(p)$ and $(t, p) = 1$.*

(a) If $p \equiv 1 \pmod{2ru}$, then

$$\sigma_\omega(sp + tn) = \frac{2}{ru} \sum_{j=1}^{u/2} \begin{pmatrix} g_{ru/2}(\omega^j t) - 1 & 0 \\ 0 & g_{ru}(\omega^j t) - g_{ru/2}(\omega^j t) \end{pmatrix} \sigma_{\omega_n^u}(\omega^j s).$$

(b) If $4|u$ *and* $p \equiv 1 + \frac{ru}{2} \pmod{ru}$*, then*

$$\sigma_\omega(sp+tn) = \frac{4}{ru}\sum_{j=1}^{u/2} \begin{pmatrix} \Re(g_{ru/2}(\omega^j t)) - 1 & 0 \\ \Im(g_{ru/2}(\omega^j t)) & 0 \end{pmatrix} \sigma_{\omega_n^u}(\omega^j s).$$

Proof. We show (a) in detail and describe an analogous proof of (b). In either setting, since v is odd, the set of residues of the form $\omega_n^{u/2}\omega_n^{uj}$ for $j = 1, \ldots, v$ is equal to the set of residues of the form $\omega_n^{uv/2}\omega_n^{uj} = -\omega_n^{uj}$. Hence

$$\sigma_{\omega_n^u}(\omega^{u/2}s) = \sum_{j=1}^{v} e\left(\frac{\omega^{u/2}\omega^{uj}}{n}\right) = \sum_{j=1}^{v} e\left(\frac{-\omega^{uj}}{n}\right) = \overline{\sigma_{\omega_n^u}(s)} \tag{8}$$

for all s. Suppose now that $p \equiv 1 \pmod{2ru}$, as in (i). Lemma 3.5 says that

$$\sigma_\omega(sp+tn) = \frac{1}{ru}\sum_{j=1}^{uv}(g_{ru}(\omega^j t) - 1)\sigma_{\omega_n^u}(\omega^j s),$$

where, by (8) and Lemma 3.6, we have

$$\begin{aligned}&(g_{ru}(\omega^j t) - 1)\sigma_{\omega_n^u}(\omega^j s) + (g_{ru}(\omega^{j+u/2}t) - 1)\sigma_{\omega_n^u}(\omega^{j+u/2}s) \\ &\quad = \begin{pmatrix} g_{ru}(\omega^j t) + g_{ru}(\omega^{j+u/2}t) - 2 & 0 \\ 0 & g_{ru}(\omega^j t) - g_{ru}(\omega^{j+u/2}t) \end{pmatrix} \sigma_{\omega_n^u}(\omega^j s), \end{aligned} \tag{9}$$

for $j = 1, \ldots, \frac{u}{2}$. Let χ be the character mod p of order ru with $\chi(\omega) = e(\frac{1}{u})$, and notice that

$$g_{ru}(\omega^{u/2}t) = \sum_{j=1}^{ru-1} G(\omega^{u/2}t, \chi^j) = \sum_{j=1}^{ru-1} \chi^j(\omega^{-u/2})G(t, \chi^j) = \sum_{j=1}^{ru-1} (-1)^j G(t, \chi^j).$$

It follows that

$$g_{ru}(t) + g_{ru}(\omega^{u/2}t) = \sum_{j=1}^{ru-1} G(t, \chi^j) + (-1)^j G(t, \chi^j) = 2g_{ru/2}(t), \tag{10}$$

which gives

$$g_{ru}(t) - g_{ru}(\omega^{u/2}t) = 2(g_{ru}(t) - g_{ru/2}(t)).$$

Combining this with (9) and (10) completes the proof of (a). The argument for (b) is similar in spirit to the one just given, with the main differences being that $\sigma_{\omega_p^u} = g_{ru/2}$ and $g_{ru/2}(\omega^{u/2}t) = g_{ru/2}(t)$ for all t. □

Certain families of real-valued cyclic supercharacters, while less interesting from a visual standpoint, can also be described by Theorem 3.2. The following proposition describes two. We omit the proof, which resembles the previous one.

Proposition 3.8. *Suppose, in addition to the hypotheses of Lemma 3.5, that* v *is odd and* $\omega_n^{uv/2} = -1$*.*

(a) If $u = 2$ *and* $p \equiv 3 \pmod 4$*, then*

$$\sigma_\omega(sp+tn) = \begin{pmatrix} -1 & -\chi(t)\sqrt{p} \\ 0 & 0 \end{pmatrix} \sigma_{\omega_n^2}(s).$$

(b) Suppose that $p \equiv 5 \pmod 8$, and let χ be the unique character mod p with $\chi(\omega) = i$. If $u = 4$, then

$$\sigma(sp+tn) = \begin{pmatrix} \frac{1}{2}(g_2(t)-1) & \Re(G(t,\chi)) \\ 0 & 0 \end{pmatrix} \sigma_{\omega_n^4}(s) + \begin{pmatrix} \frac{1}{2}(-g_2(t)-1) & \Im(G(t,\chi)) \\ 0 & 0 \end{pmatrix} \sigma_{\omega_n^4}(\omega s).$$

4. Examples

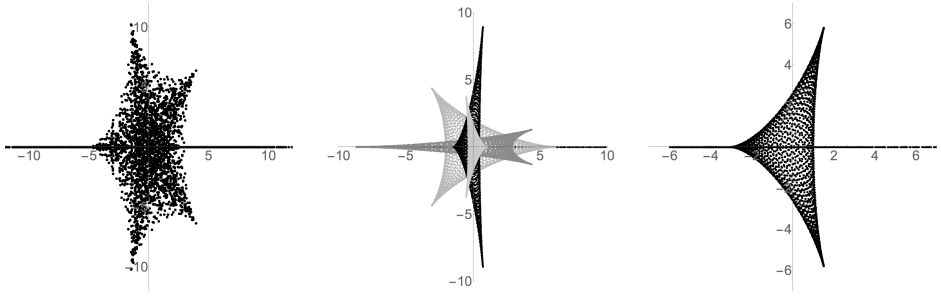
The images of cyclic supercharacters σ_ω satisfying the hypotheses of Theorem 3.7 belong to Minkowski sums of $\mathrm{im}(\sigma_{\omega_n})$ where each summand is subject to an $\mathbb{R}$-linear transformation. This observation informs our perspective in what follows.

For a positive integer a, a divisor b of a, and a unit ω mod a, the sets

$$\{\sigma_\omega(y) : y \equiv j \pmod b\}$$

for $j = 0, 1, \ldots, b-1$ are called the *layers mod b* of σ_ω. The layer mod b corresponding to $j = 0$ is called *trivial*. Different shades of points plotted in Figures 1, 6(B), 8(B), 10(B), 11(A) and 11(B) mark distinct layers of the corresponding cyclic supercharacters. That is, in each figure, if $y \equiv y' \pmod b$ for some fixed divisor b of the modulus, then $\sigma_\omega(y)$ and $\sigma_\omega(y')$ have the same shade. Under the hypotheses of Theorem 3.7, σ_ω has $r+1$ distinct layers mod p, the trivial one of which is the subset of $\mathbb{R}$ consisting of all values $\sigma_\omega(sp+tn)$ for which $p|t$.

4.1. **Stretching.** In the following, we assume the hypotheses of Theorem 3.7(a), where the $\mathbb{R}$-linear transformations discussed above are scalings along the real and imaginary axes, possibly by negative factors. When n is an odd prime distinct from p and v is a power of an odd prime, the discussion in Section 2 tells us that the corresponding images $\mathrm{im}(\omega_\omega)$ can be arranged in sequences filling out Minkowski sums of stretched versions of H_r. Figure 6 illustrates this behavior.



(A) $(5, 13291, 8142)$ (B) $(17, 6493, 27213)$ (C) $(5, 6247, 2317)$

FIGURE 6. For the given triples (p, n, ω), the images of the cyclic supercharacters σ_ω mod pn are explained by Theorem 3.7(a). See Section 4.1 for details.

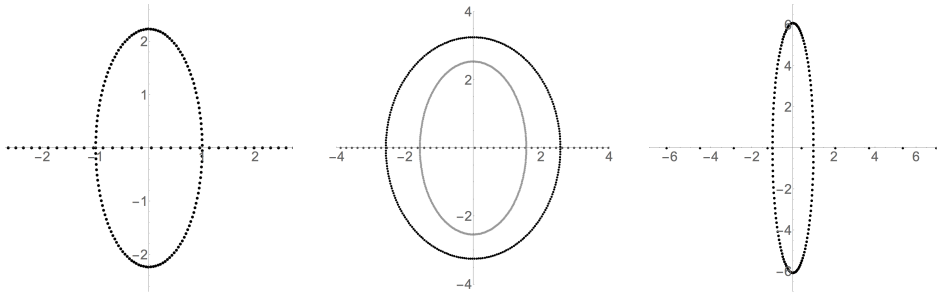
On the other hand, if $v = 1$ for any n, ellipses emerge. For the remainder of the subsection, suppose that $v = 1$. We see that

$$\sigma_\omega(sp + tn) = \frac{2}{ru} \sum_{j=1}^{u/2} \begin{pmatrix} g_{ru/2}(\omega^j t) - 1 & 0 \\ g_{ru}(\omega^j t) - g_{ru/2}(\omega^j t) & 0 \end{pmatrix} e\left(\frac{s}{n}\right).$$

Here, $\sigma_\omega(sp + tn)$ belongs to a Minkowski sum of ellipses in standard form:

$$\bigoplus_{j=1}^{u/2} \left\{ z \in \mathbb{C} : \frac{\Re(z)^2}{(g_{ru/2}(\omega^j t) - 1)^2} + \frac{\Im(z)^2}{(g_{ru}(\omega^j t) - g_{ru/2}(\omega^j t))^2} = 1 \right\}.$$

Take, for example, the case $u = 2$ and $r = 1$. In this situation, the nontrivial layer of σ_ω mod p is contained in the ellipse with equation $\Re(z)^2 + \Im(z)^2/p = 1$. This behavior, depicted by Figures 7(A) and 7(C), was first noted in [7, Proposition 5.2], but the framework here is more general. In particular, it is apparent now that such examples are more common than previously thought. Figure 7(B) illustrates the case $u = r = 2$ and, accordingly, features $r = 2$ distinct ellipses.



(A) $(5, 137, 273)$ (B) $(17, 269, 1613)$ (C) $(37, 137, 684)$

FIGURE 7. For the given triples (p, n, ω), discretized versions of ellipses appear in the plots of cyclic supercharacters σ_ω mod pn. See Section 4.1 for details.

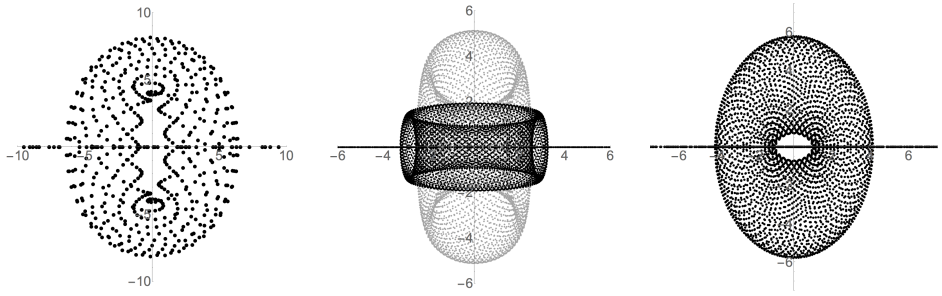
Suppose now that $u = 4$ and $r = 1$, and that χ is a character mod p of order 4. It can be shown that each nontrivial layer of σ_ω mod p is contained in the image of the $\operatorname{lcm}(2, n)$-th roots of unity under the map

$$z \mapsto \begin{pmatrix} \frac{1}{2}(\sqrt{p} - 1) & 0 \\ 0 & \Re(G(\chi)) \end{pmatrix} z + \begin{pmatrix} \frac{1}{2}(\sqrt{p} + 1) & 0 \\ 0 & \Im(G(\chi)) \end{pmatrix} z^\omega,$$

which can be rewritten to reflect the fact that $|G(\chi)| = \sqrt{p}$. The image in question is most easily visualized as the path of a point winding ω times around an ellipse whose center travels once around another ellipse. Figures 8(A) and 8(C) depict this behavior, while Figure 8(B), which appeared in [7] unexplained, illustrates the case $u = 4$ and $r = 2$.

Returning to the case $u = 2$, suppose now that r is maximal, i.e., $r = \frac{\varphi(p)}{4}$. Each of the r nontrivial layers of σ_ω is the image of the set of $\operatorname{lcm}(2, n)$-th roots of unity under $\mathbb{R}$-linear map with matrix

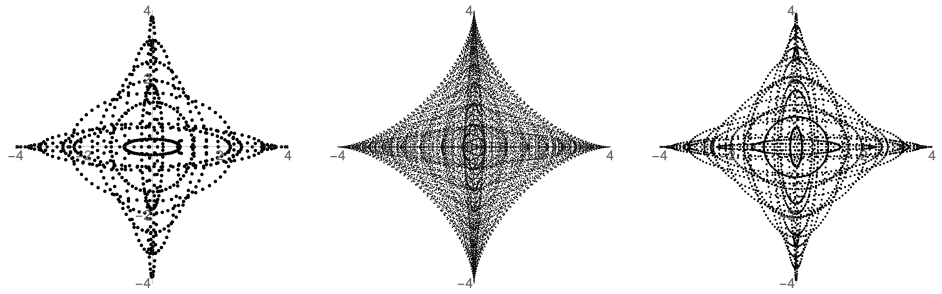
$$\begin{pmatrix} \cos(2\pi t/n) + \cos(2\pi\omega t/n) & 0 \\ 0 & \cos(2\pi t/n) - \cos(2\pi\omega t/n) \end{pmatrix},$$



(A) $(41, 541, 52)$ (B) $(17, 5365, 2337)$ (C) $(17, 3581, 364)$

FIGURE 8. For the given triples (p, n, ω), the ovate figures contained in the plots of the cyclic supercharacters σ_ω mod pn are the effect of one ellipse "winding around" another. See Section 4.1 for details.

for some t coprime to p. This image, in turn, belongs to an ellipse whose semimajor and semiminor axes sum to at most 4. The envelope of the family of all such ellipses is the boundary of H_4. Accordingly, for large p, plots of these cyclic supercharacters tend to resemble H_4. Figure 9 presents several examples.



(A) $(59, 53, 235)$ (B) $(19, 3617, 1234)$ (C) $(107, 109, 1711)$

FIGURE 9. For the given triples (p, n, ω), the plots of the cyclic supercharacters σ_ω mod pn contain discretized ellipses within H_4.

4.2. **Rhombi.** For this section, we assume the hypotheses of Theorem 3.7(b), and additionally that $u = 4$ and $v = 1$. A routine computation gives $g_{2r}(\omega t) = \overline{g_{2r}(t)}$ for all t, so

$$\sigma_\omega(sp + tn) = \frac{1}{r}\begin{pmatrix} \Re(g_{2r}(t)) - 1 & 0 \\ \Im(g_{2r}(t)) & 0 \end{pmatrix} e\left(\frac{s}{n}\right) + \frac{1}{r}\begin{pmatrix} \Re(g_{2r}(t)) - 1 & 0 \\ -\Im(g_{2r}(t)) & 0 \end{pmatrix} e\left(\frac{\omega s}{n}\right).$$

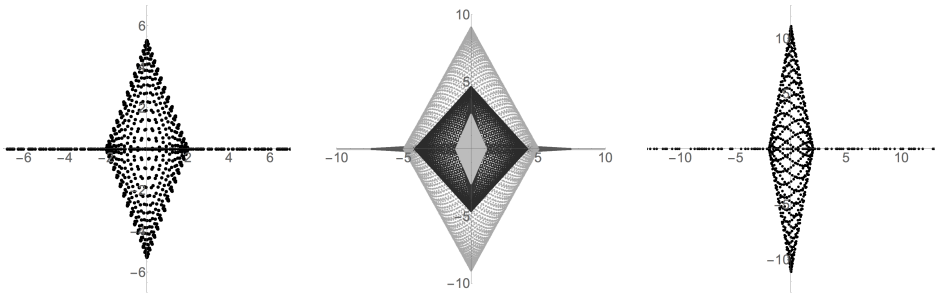
We claim that scaling the real and imaginary parts of $\sigma_\omega(sp + tn)$ by factors dependent only on t and rotating counterclockwise by $\frac{\pi}{2}$ about the origin yields a point with real and imaginary parts each in the interval $[-1, 1]$. Indeed, consider the $\mathbb{R}$-linear map on $\mathbb{C}$ with matrix

$$T = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} \frac{\sqrt{2}}{r}(\Re(g_{2r}(t)) - 1) & 0 \\ 0 & \frac{\sqrt{2}}{r}\Im(g_{2r}(t)) \end{pmatrix}^{-1},$$

and notice that

$$T\sigma_\omega(sp+tn) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} e\left(\frac{s}{n}\right) + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} e\left(\frac{\omega s}{n}\right).$$

It follows that each nontrivial layer of σ_ω mod p is contained in the convex hull of a rhombus in $\mathbb{C}$ with vertices at $\pm\frac{2}{r}(\Re(g_{2r}(t)) - 1)$ and $\pm i\frac{2}{r}\Im(g_{2r}(t))$ for some t coprime to p. Plots of these cyclic supercharacters appear in both [7] and [12]. In case $r = 1$, as in Figures 10(A) and 10(C), the vertices of the sole rhombus are at ± 2 and $\pm 2i\sqrt{p}$. Figure 10(B) illustrates the case $r = 5$.



(A) $(7, 1229, 3055)$ (B) $(31, 11849, 24527)$ (C) $(31, 1429, 809)$

FIGURE 10. For the given triples (p, n, ω), the nontrivial layers of the cyclic supercharacters σ_ω mod pn are contained in rhombi. See Section 4.2 for details.

5. The present unknown

While Theorem 3.7 provides concrete explanations of certain graphical behaviors, many remain elusive. It seems likely, however, that more could be handled in similar fashion to the ones above, armed with Theorem 3.2 and the language of Minkowski addition and multiplication. To close, we present Figure 11, which provides a small gallery of plots yet unexplained. In Figure 11(A), the nontrivial layers appear to be contained in Minkowski sums of 3 line segments. The nontrivial layers in Figure 11(B) suggest Minkowski sums of ellipses, as in Section 4.1. Patterns resembling the one in Figure 11(C), where $n = 524287$ and $\omega = 2$, seem to occur whenever n has the form $2^j - 1$ and $\omega = 2$. We leave the reader with these observations.

Appendix

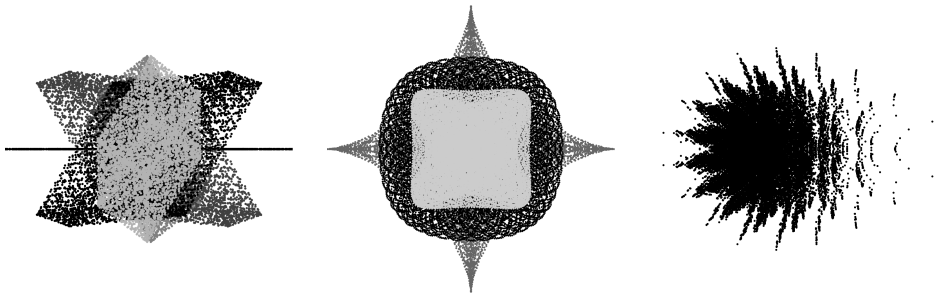
We dedicate this section to proving Proposition 3.4. For $A \subset \mathbb{C}$, define the *backward cone* of A to be the set $C(A)$ given by

$$C(A) = \{\lambda z \in \mathbb{C} : \lambda \in [0, 1] \text{ and } z \in A\}.$$

If A is compact, we define its *outer boundary* $\partial(A)$ by

$$\partial(A) = \{z \in A : A \cap \{\lambda z : \lambda > 1\} = \emptyset\}.$$

Notice that if A is compact, then $\partial(A) = \partial(C(A))$, and that if B is also compact, then $\partial(A \otimes B) \subset \partial(\partial(A) \otimes \partial(B))$, with equality if A and B are star shaped with center 0.



(A) $n = 398157$, $\omega = 1070$ (B) $n = 546975$, $\omega = 593$ (C) $n = 524287$, $\omega = 2$

FIGURE 11. The plots of these cyclic supercharacters σ_ω mod n have yet to be explained.

Proof of Proposition 3.4. Let E_k (resp., E_ℓ) be the edge of the polygon $\partial(P_k)$ (resp., $\partial(P_\ell)$) perpendicular to the real axis. By the preceding discussion, we see that

$$\begin{aligned}\partial(P_k \otimes P_\ell) &= \partial(P_k) \otimes \partial(P_\ell) \\ &= \partial(\{e(\tfrac{j}{k\ell}) : j = 1, \ldots, k\ell\} \otimes (E_k \otimes E_\ell)) \\ &\subset \{e(\tfrac{j}{k\ell}) : j = 1, \ldots, k\ell\} \otimes \partial(E_k \otimes E_\ell) \\ &= \{e(\tfrac{j}{k\ell}) : j = 1, \ldots, k\ell\} \otimes \partial(C(E_k \otimes E_\ell)). \end{aligned} \tag{11}$$

Let $a_k = -k\cos\frac{\pi}{k}$ (resp., $a_\ell = -\ell\cos\frac{\pi}{\ell}$), so that $a_k^{-1}E_k$ (resp., $a_\ell^{-1}E_\ell$) is the line segment connecting $1 \pm i\tan\frac{\pi}{k}$ (resp., $1 \pm i\tan\frac{\pi}{\ell}$). By [16, Theorem 2.4(c)], $C(a_k^{-1}E_k \otimes a_\ell^{-1}E_\ell)$ is the set illustrated in Figure 12, where

$$\begin{aligned} z_1 &= 1 + \tan^2\tfrac{\pi}{\ell} \\ z_2 &= 1 + \tan\tfrac{\pi}{k}\tan\tfrac{\pi}{\ell} + i(\tan\tfrac{\pi}{k} - \tan\tfrac{\pi}{\ell}) \\ z_3 &= 1 - \tan\tfrac{\pi}{k}\tan\tfrac{\pi}{\ell} + i(\tan\tfrac{\pi}{k} + \tan\tfrac{\pi}{\ell}). \end{aligned}$$

Since $C(E_k \otimes E_\ell) = a_k a_\ell C(a_k^{-1}E_k \otimes a_\ell^{-1}E_\ell)$, the result follows from combining standard trigonometric identities with (11) and (3). □

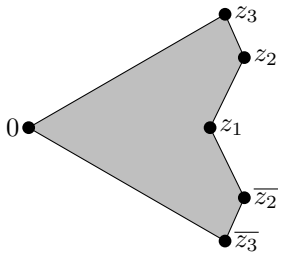


FIGURE 12. The set $C(a_k^{-1}E_k \otimes a_\ell^{-1}E_\ell)$ defined in the proof of Proposition 3.4.

References

1. Leonard D. Baumert, *Cyclic difference sets*, Springer, 1971.
2. Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and jacobi sums*, Canadian Mathematical Society series of monographs and advanced texts, Wiley, 1998.
3. J.L. Brumbaugh, Madeleine Bulkow, Patrick S. Fleming, Luis Alberto Garcia German, Stephan Ramon Garcia, Gizem Karaali, Matt Michal, Andrew P. Turner, and Hong Suh, *Supercharacters, exponential sums, and the uncertainty principle*, J. Number Theory **144** (2014), 151–175.
4. Paula Burkhardt, Alice Zhuo-Yu Chan, Gabriel Currier, Stephan Ramon Garcia, Florian Luca, and Hong Suh, *Visual properties of generalized Kloosterman sums*, J. Number Theory **160** (2016), 237–253.
5. Barrie Cooper, *Almost Koszul duality and rational conformal field theory*, Ph.D. thesis, University of Bath, July 2007.
6. Persi Diaconis and I.M. Isaacs, *Supercharacters and superclasses for algebra groups*, Trans. Amer. Math. Soc. **360** (2008), no. 5, 2359–2392.
7. William Duke, Stephan Ramon Garcia, and Bob Lutz, *The graphic nature of Gaussian periods*, Proc. Amer. Math. Soc. **143** (2015), no. 5.
8. Ronald J. Evans, *Generalized cyclotomic periods*, Proc. Amer. Math. Soc. **81** (1981), no. 2, 207–212 (English).
9. ———, *Period polynomials for generalized cyclotomic periods*, Manuscripta Math. **40** (1982), no. 2-3, 217–243.
10. Rida T. Farouki, Hwan Pyo Moon, and Bahram Ravani, *Algorithms for Minkowski products and implicitly-defined complex sets*, Adv. Comput. Math. **13** (2000), no. 3, 199–229.
11. ———, *Minkowski geometric algebra of complex sets*, Geom. Dedicata **85** (2001), no. 1, 283–315.
12. Stephan Ramon Garcia, Mark Huber, and Bob Lutz, *A supercharacter approach to Heilbronn sums*, arXiv preprint arXiv:1312.1034 (2015).
13. Trevor Hyde, Stephan Ramon Garcia, and Bob Lutz, *Gauss's hidden menagerie: from cyclotomy to supercharacters*, Notices Amer. Math. Soc. **62** (2015), no. 8, 878–888.
14. D.H. Lehmer and Emma Lehmer, *Cyclotomy for non-squarefree moduli*, Analytic Number Theory (Marvin I. Knopp, ed.), Lecture Notes in Math., vol. 899, Springer, 1981, pp. 276–300.
15. H.W. Lenstra, *Primality testing with Gaussian periods*, FST TCS 2002: Foundations of Software Technology and Theoretical Computer Science (Manindra Agrawal and Anil Seth, eds.), Lecture Notes in Computer Science, vol. 2556, Springer Berlin Heidelberg, 2002, pp. 1–1 (English).
16. Chi-Kwong Li, Diane Christine Pelejo, Yiu-Tung Poon, and Kuo-Zhong Wang, *Minkowski product of convex sets and product numerical range*, Oper. Matrices, to appear.
17. Ross M. Starr, *Quasi-equilibria in markets with non-convex preferences*, Econometrica **37** (1969), no. 1, 25–38.

Department of Mathematics, University of Michigan, 2074 East Hall, 530 Church Street, Ann Arbor, MI 48109, USA

E-mail address: boblutz@umich.edu

URL: http://www-personal.umich.edu/~boblutz