THE GRAPHIC NATURE OF GAUSSIAN PERIODS

WILLIAM DUKE, STEPHAN RAMON GARCIA, AND BOB LUTZ

Abstract. Recent work has shown that the study of supercharacters on abelian groups provides a natural framework within which to study certain exponential sums of interest in number theory. Our aim here is to initiate the study of Gaussian periods from this novel perspective. Among other things, our approach reveals that these classical objects display dazzling visual patterns of great complexity and remarkable subtlety.

1. Introduction

The theory of supercharacters, which generalizes classical character theory, was recently introduced in an axiomatic fashion by P. Diaconis and I.M. Isaacs [6], extending the seminal work of C. André [1, 2]. Recent work has shown that the study of supercharacters on abelian groups provides a natural framework within which to study the properties of certain exponential sums of interest in number theory [4, 8] (see also [7] and Table 1). Our aim here is to initiate the study of Gaussian periods from this novel perspective. Among other things, this approach reveals that these classical objects display a dazzling array of visual patterns of great complexity and remarkable subtlety (see Figure 1).

Let G be a finite group with identity 0, $\mathcal{K}$ a partition of G, and $\mathcal{X}$ a partition of the set $\operatorname{Irr}(G)$ of irreducible characters of G. The ordered pair $(\mathcal{X}, \mathcal{K})$ is called a *supercharacter theory* for G if $\{0\} \in \mathcal{K}$, $|\mathcal{X}| = |\mathcal{K}|$, and for each $X \in \mathcal{X}$, the function

$$\sigma_X = \sum_{\chi \in X} \chi(0)\chi$$

is constant on each $K \in \mathcal{K}$. The functions σ_X are called *supercharacters* of G and the elements of $\mathcal{K}$ are called *superclasses*.

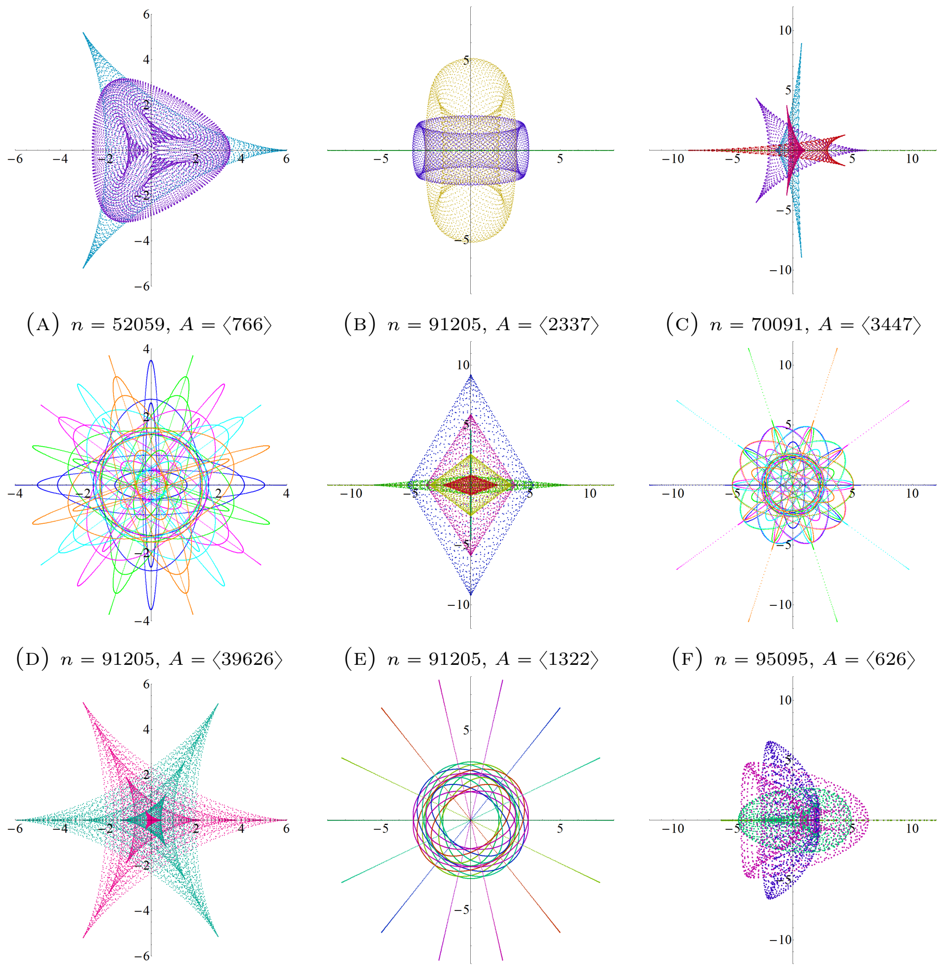
Let $G = \mathbb{Z}/n\mathbb{Z}$ and recall that the irreducible characters of $\mathbb{Z}/n\mathbb{Z}$ are the functions $\chi_x(y) = e(\frac{xy}{n})$ for x in $\mathbb{Z}/n\mathbb{Z}$, where $e(\theta) = \exp(2\pi i\theta)$. For a fixed subgroup A of $(\mathbb{Z}/n\mathbb{Z})^\times$, let $\mathcal{K}$ denote the partition of $\mathbb{Z}/n\mathbb{Z}$ arising from the action $a \cdot x = ax$ of A. The action $a \cdot \chi_x = \chi_{a^{-1}x}$ of A on the irreducible characters of $\mathbb{Z}/n\mathbb{Z}$ yields a compatible partition $\mathcal{X}$. The reader can verify that $(\mathcal{X}, \mathcal{K})$ is a supercharacter theory on $\mathbb{Z}/n\mathbb{Z}$ and that the corresponding supercharacters are given by

$$\sigma_X(y) = \sum_{x \in X} e\left(\frac{xy}{n}\right), \tag{1}$$

where X is an orbit in $\mathbb{Z}/n\mathbb{Z}$ under the action of A. When $n = p$ is an odd prime, (1) is a *Gaussian period*, a central object in the theory of cyclotomy. For $p = kd + 1$, Gauss defined the *d-nomial periods* $\eta_j = \sum_{\ell=0}^{d-1} \zeta_p^{g^{k\ell+j}}$, where $\zeta_p = e(\frac{1}{p})$ and g denotes a primitive root modulo p [3, 5]. Clearly η_j runs over the same values as

Partially supported by National Science Foundation Grants DMS-10-01527, DMS-1001614, and DMS-1265973.

$\sigma_X(y)$ when $y \neq 0$, $|A| = d$, and $X = A1$ is the A-orbit of 1. For composite moduli, the functions σ_X attain values which are generalizations of Gaussian periods of the type considered by Kummer and others (see [10]).



(A) $n = 52059,\ A = \langle 766 \rangle$ (B) $n = 91205,\ A = \langle 2337 \rangle$ (C) $n = 70091,\ A = \langle 3447 \rangle$

(D) $n = 91205,\ A = \langle 39626 \rangle$ (E) $n = 91205,\ A = \langle 1322 \rangle$ (F) $n = 95095,\ A = \langle 626 \rangle$

(G) $n = 82677,\ A = \langle 8147 \rangle$ (H) $n = 70091,\ A = \langle 21792 \rangle$ (I) $n = 51319,\ A = \langle 430 \rangle$

FIGURE 1. Each subfigure is the image of $\sigma_X : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$, where X is the orbit of 1 under the action of a cyclic subgroup A of $(\mathbb{Z}/n\mathbb{Z})^\times$. If $\sigma_X(y)$ and $\sigma_X(y')$ differ in color, then $y \not\equiv y' \pmod{m}$, where m is a fixed divisor of n.

When visualized as subsets of the complex plane, the images of these supercharacters exhibit a surprisingly diverse range of features (see Figure 1). The main purpose of this paper is to initiate the investigation of these plots, focusing our attention on the case where $A = \langle a \rangle$ is a cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. We refer to supercharacers which arise in this manner as *cyclic supercharacters*.

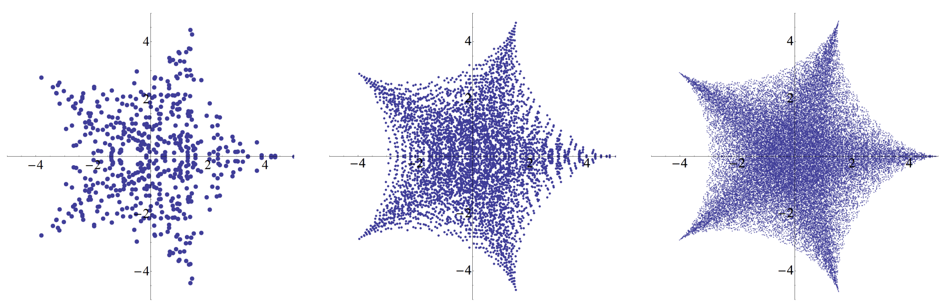
The sheer diversity of patterns displayed by cyclic supercharacters is overwhelming. To some degree, these circumstances force us to focus our initial efforts on documenting the notable features that appear and on explaining their number-theoretic origins. One such theorem is the following.

Name	Expression	G	A
Gauss	$\eta_j = \sum_{\ell=0}^{d-1} e\left(\frac{g^{k\ell+j}}{p}\right)$	$\mathbb{Z}/p\mathbb{Z}$	nonzero kth powers mod p
Ramanujan	$c_n(x) = \sum_{\substack{j=1 \\ (j,n)=1}}^{n} e\left(\frac{jx}{n}\right)$	$\mathbb{Z}/n\mathbb{Z}$	$(\mathbb{Z}/n\mathbb{Z})^\times$
Kloosterman	$K_p(a,b) = \sum_{\ell=0}^{p-1} e\left(\frac{a\ell + b\bar{\ell}}{p}\right)$	$(\mathbb{Z}/p\mathbb{Z})^2$	$\left\{\begin{bmatrix} u & 0 \\ 0 & u^{-1}\end{bmatrix} : u \in (\mathbb{Z}/p\mathbb{Z})^\times\right\}$
Heilbronn	$H_p(a) = \sum_{\ell=0}^{p-1} e\left(\frac{a\ell^p}{p^2}\right)$	$\mathbb{Z}/p^2\mathbb{Z}$	nonzero pth powers mod p^2

TABLE 1. Gaussian periods, Ramanujan sums, Kloosterman sums, and Heilbronn sums appear as supercharacters arising from the action of a subgroup A of $\operatorname{Aut} G$ for a suitable abelian group G. Here p denotes an odd prime number.

Theorem 1.1. *Suppose that $q = p^a$ is an odd prime power and that σ_X is a cyclic supercharacter of $\mathbb{Z}/q\mathbb{Z}$. If $|X| = d$ is prime and $d \neq p$, then the image of σ_X is bounded by the d-cusped hypocycloid parametrized by $\theta \mapsto (d-1)e^{i\theta} + e^{i(d-1)\theta}$.*

In fact, for a fixed prime m, as the modulus $q \equiv 1 \pmod{d}$ tends to infinity the corresponding supercharacter images become dense in the filled hypocycloid in a sense that will be made precise in Section 6 (see Figures 2 and 9).



(A) $p = 2791,\ A = \langle 800 \rangle$ (B) $p = 27011,\ A = \langle 9360 \rangle$ (C) $p = 202231,\ A = \langle 61576 \rangle$

FIGURE 2. Graphs of cyclic supercharacters $\sigma_X : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ where $X = A1$.

The preceding result is itself a special case of a much more general theorem (Theorem 6.3) which relates the asymptotic behavior of cyclic supercharacter plots to the mapping properties of certain multivariate Laurent polynomials, regarded as complex-valued functions on suitable high-dimensional tori.

2. Multiplicativity and nesting plots

Our first order of business is to determine when and in what manner the image of one cyclic supercharacter plot can appear in another. Certain cyclic supercharacters have a naturally multiplicative structure. When combined with Proposition 2.4 and the discussion in Section 6, the following result provides a complete picture of these supercharacters. Following the introduction, we let $X = Ar$ denote the orbit of r in $\mathbb{Z}/n\mathbb{Z}$ under the action of a cyclic subgroup A of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem 2.1. *Let σ_X be a cyclic supercharacter of $\mathbb{Z}/n\mathbb{Z}$, writing $n = \prod_{j=1}^k p_j^{a_j}$ in standard form and $X = \langle\omega\rangle$. For each j, let $\psi_j : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p_j^{a_j}\mathbb{Z}$ be the natural homomorphism, let x_j be the multiplicative inverse of $n/p_j^{a_j} \pmod{p_j^{a_j}}$, and write $X_j = \langle\psi_j(\omega)\rangle x_j\psi_j(r)$. If the orbit sizes $|X_j|$ are pairwise coprime, then*

$$\sigma_X(y) = \prod_{j=1}^k \sigma_{X_j}\big(\psi_j(y)\big).$$

Proof. We prove the theorem for $n = p_1p_2$ a product of distinct primes; the general argument is similar. Let $\psi = (\psi_1, \psi_2)$ be the ring isomorphism given by the Chinese Remainder Theorem, and let $d = |X|$, $d_1 = |\psi_1(X)|$ and $d_2 = |\psi_2(X)|$. We have

$$\begin{aligned}
\sigma_{X_1}\big(\psi_1(y)\big)\sigma_{X_2}\big(\psi_2(y)\big) &= \sum_{j=0}^{d_1-1} e\left(\frac{\psi_1(\omega^j ry)x_1}{p_1}\right)\sum_{k=0}^{d_2-1} e\left(\frac{\psi_2(\omega^k ry)x_2}{p_2}\right)\\
&= \sum_{j=0}^{d_1-1}\sum_{k=0}^{d_2-1} e\left(\frac{\psi_1(\omega^j ry)x_1}{p_1} + \frac{\psi_2(\omega^k ry)x_2}{p_2}\right)\\
&= \sum_{j=0}^{d_1-1}\sum_{k=0}^{d_2-1} e\left(\frac{\psi^{-1}\big(\psi_1(\omega^j ry), \psi_2(\omega^k ry)\big)}{n}\right)\\
&= \sum_{j=0}^{d_1-1}\sum_{k=0}^{d_2-1} e\left(\frac{\psi^{-1}\big(\psi_1(\omega)^j, \psi_2(\omega)^k\big)ry}{n}\right)\\
&= \sum_{\ell=0}^{d-1} e\left(\frac{\omega^\ell ry}{n}\right)\\
&= \sigma_X(y).
\end{aligned}$$

□

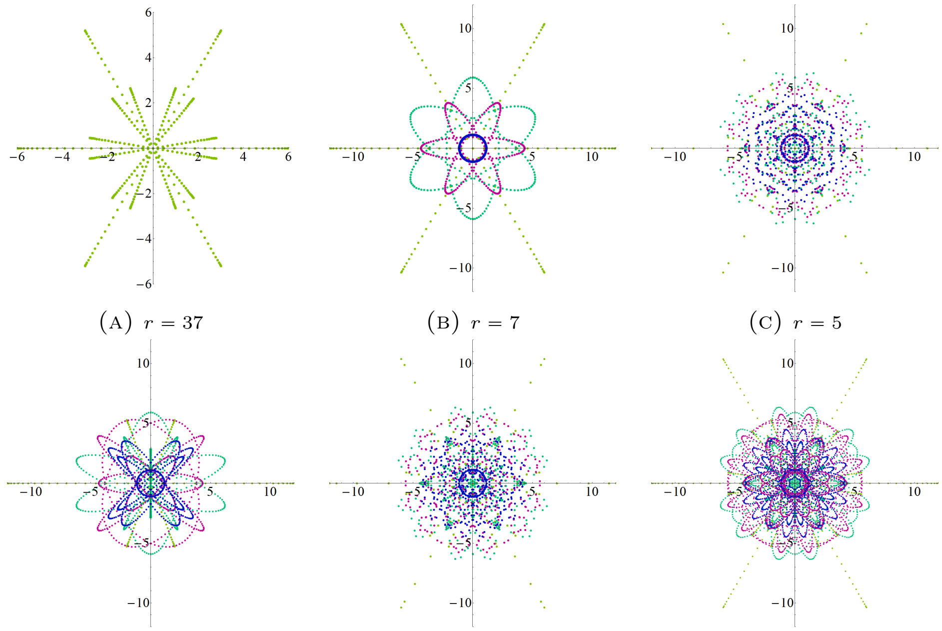
The following easy result tells us that we observe all possible graphical behavior, up to scaling, by studying cases where $r = 1$ (i.e., where $X = A$ as sets).

Proposition 2.2. *Let r belong to $\mathbb{Z}/n\mathbb{Z}$, and suppose that $(r, n) = \frac{n}{d}$ for some positive divisor d of n, so that $\xi = \frac{rd}{n}$ is a unit modulo n. Also let $\psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ be the natural homomorphism.*

(i) *The images of σ_{Ar}, $\sigma_{A(r,n)}$, and $\sigma_{\psi_d(A)1}$ are equal.*

(ii) *The image in (i), when scaled by $\frac{|A|}{|\psi_d(A)|}$, is a subset of the image of $\sigma_{A\xi}$.*

Example 2.3. Let $n = 62160 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 37$. Each plot in Figure 3 displays the image of a different cyclic supercharacter σ_X, where $X = \langle 319\rangle r$. If $d = r/(n, r)$, then Proposition 2.2(i) says that each image equals that of a cyclic supercharacter $\sigma_{X'}$ of $\mathbb{Z}/d\mathbb{Z}$, where $X' = \langle\psi_d(319)\rangle 1$. Proposition 2.2(ii) says that each nests in the image in Figure 3(F).



(A) $r = 37$ (B) $r = 7$ (C) $r = 5$

(D) $r = 3$ (E) $r = 4$ (F) $r = 1$

FIGURE 3. Graphs of cyclic supercharacters σ_X of $\mathbb{Z}/62160\mathbb{Z}$, where $X = \langle 319 \rangle r$. Each image nests in Figure 3(F), as per Proposition 2.2(ii). See Figure 1 for a brief discussion of colorization.

Because of Theorem 2.1, we are mostly interested in prime power moduli. The following result implies that the image of any cyclic supercharacter on $\mathbb{Z}/p^a\mathbb{Z}$ is a scaled copy of one whose boundary is given by Theorem 6.3.

Proposition 2.4. *Let p be an odd prime, $a > b$ nonnegative integers, and ψ the natural homomorphism from $\mathbb{Z}/p^a\mathbb{Z}$ to $\mathbb{Z}/p^{a-b}\mathbb{Z}$. If σ_X is a cyclic supercharacter of $\mathbb{Z}/p^{a-b}\mathbb{Z}$, where $X = A1$ with $p^b \big| |X|$ and $p^{a-b} \equiv 1 \pmod{|\varphi(X)|}$, then*

$$\sigma_X(\mathbb{Z}/p^a\mathbb{Z}) = \{0\} \cup p^b \sigma_{\varphi(X)}(\mathbb{Z}/p^{a-b}\mathbb{Z}).$$

Proof. Let $k|(p-1)$. If $|X| = kp^b$, then $A = \psi^{-1}(A')$, where A' is the unique subgroup of $(\mathbb{Z}/p^{a-b}\mathbb{Z})^\times$ of order k. Let $X' = A'1$ (i.e., $X' = \varphi(X)$), so that

$$X = \{x + jp^{a-b} : x \in X',\ j = 0, 1, \ldots, p^b - 1\}.$$

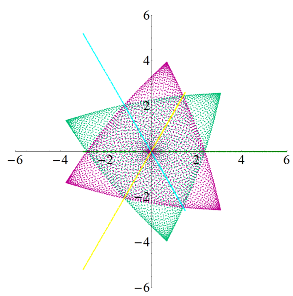
We have

$$\begin{aligned}
\sigma_X(y) &= \sum_{x \in X'} \sum_{j=0}^{p^b-1} e\left(\frac{(x + jp^{a-b})y}{p^a}\right) \\
&= \sum_{j=0}^{p^b-1} e\left(\frac{jy}{p^b}\right) \sum_{x \in X'} e\left(\frac{xy}{p^a}\right) \\
&= \begin{cases} p^b \sigma_{X'}(\psi(y)), & \text{if } p^b | y \\ 0, & \text{else.} \end{cases}
\end{aligned}$$

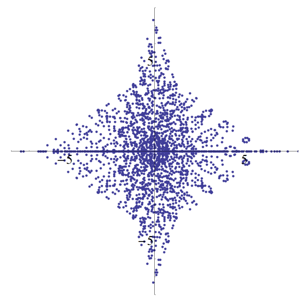
$\square$

3. Symmetries

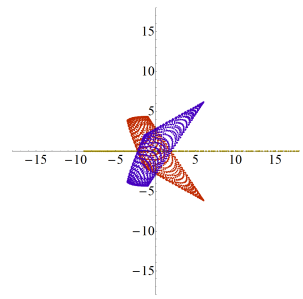
We say that a cyclic supercharacter $\sigma_X : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ has *k-fold dihedral symmetry* if its image is invariant under the natural action of the dihedral group of order $2k$. In other words, σ_X has k-fold dihedral symmetry if its image is invariant under complex conjugation and rotation by $2\pi/k$ about the origin. If X is the orbit of r, where $(r, n) = \frac{n}{d}$ for some odd divisor d of n, then σ_X is generally asymmetric about the imaginary axis, as evidenced by Figure 4.



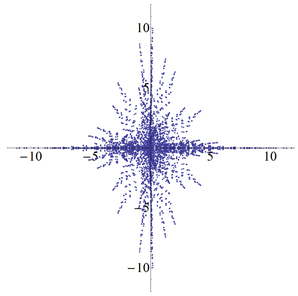
(A) $n = 68913,\ A = \langle 88 \rangle$



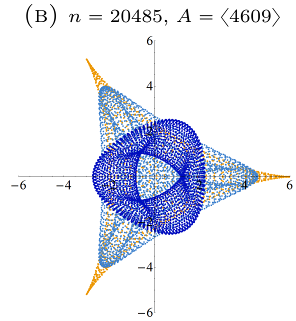
(B) $n = 20485,\ A = \langle 4609 \rangle$



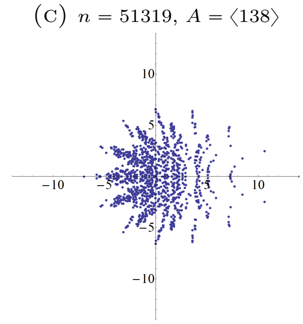
(C) $n = 51319,\ A = \langle 138 \rangle$



(D) $n = 51319,\ A = \langle 27 \rangle$



(E) $n = 44161,\ A = \langle 608 \rangle$



(F) $N = 16383,\ A = \langle 2 \rangle$

Figure 4. Graphs of $\sigma_X : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$, where $X = Ar$, fixing $r = 1$ (close inspection reveals that (E) enjoys no rotational symmetry).

Proposition 3.1. *If σ_X is a cyclic supercharacter of $\mathbb{Z}/n\mathbb{Z}$, where $X = \langle \omega \rangle r$, then σ_X has $(\omega - 1, \frac{n}{(r,n)})$-fold dihedral symmetry.*

Proof. Let $d = n/(r, n)$. If $k = (\omega - 1, d)$, then ω, and hence every element of $\langle \omega \rangle$, has the form $jk + 1$. Since $r = \xi n/d$ for some unit ξ, each x in X has the form $(\xi n/d)(jk + 1)$. If $y' = y + d/k$, then $y' - y - d/k \equiv 0 \pmod{n}$, in which case

$$\frac{\xi n}{d}(jk+1)\left(y' - y - \frac{d}{k}\right) \equiv 0 \pmod{n}.$$

It follows that

$$(jk+1)\left(\frac{\xi n}{d}(y' - y) - \frac{\xi n}{k}\right) \equiv 0 \pmod{n},$$

whence

$$\frac{\xi n}{d}(jk+1)y' \equiv \frac{\xi n}{d}(jk+1)y + \frac{\xi n}{k}(jk+1) \pmod{n}$$

$$\equiv \frac{\xi n}{d}(jk+1)y + \frac{\xi n}{k} \pmod{n},$$

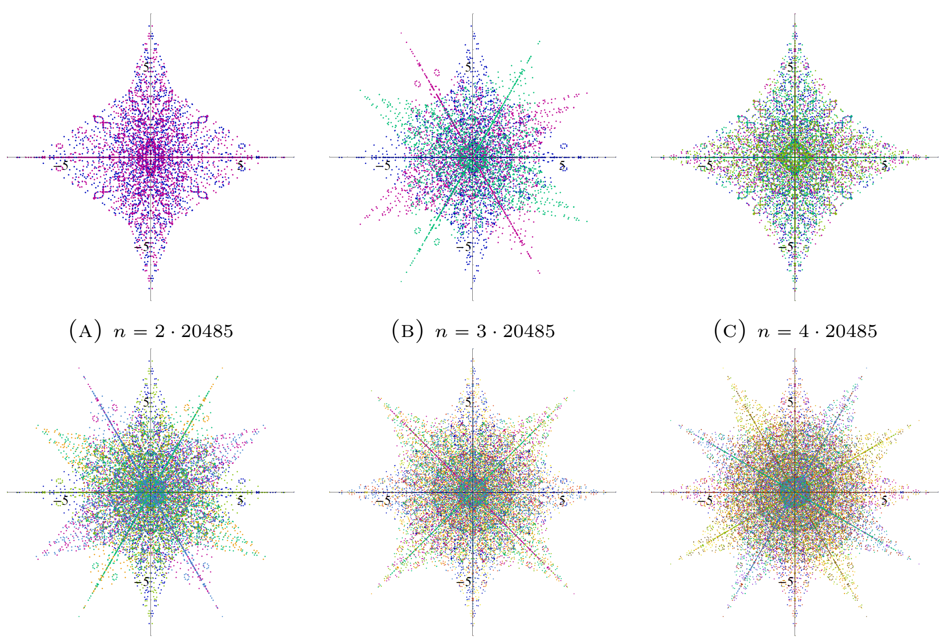
Since the function e is periodic with period 1, we have

$$\sum_{x\in X} e\left(\frac{xy'}{n}\right) = \sum_{x\in X} e\left(\frac{xy+\xi n/k}{n}\right) = e\left(\frac{\xi}{k}\right)\sum_{x\in X} e\left(\frac{xy}{n}\right).$$

In other words, the image of σ_X is invariant under counterclockwise rotation by $2\pi\xi/k$ about the origin. If $m\xi \equiv 1 \pmod{k}$, then the graph is also invariant under counterclockwise rotation by $m\cdot 2\pi\xi/k = 2\pi/k$. Dihedral symmetry follows, since for all y in $\mathbb{Z}/n\mathbb{Z}$, the the image of σ_X contains both $\sigma_X(y)$ and $\overline{\sigma_X(y)} = \sigma_X(-y)$. $\square$

Example 3.2. For $m = 1, 2, 3, 4, 6, 8, 12$, let X_m denote the orbit of 1 under the action of $\langle 4609\rangle$ on $\mathbb{Z}/(20485m)\mathbb{Z}$. Consider the cyclic supercharacter σ_{X_1}, whose graph appears in Figure 4(B). We have $(20485, 4608) = (5\cdot 17\cdot 241, 2^9\cdot 3^2) = 1$, so Theorem 3.1 guarantees that σ_{X_1} has 1-fold dihedral symmetry. It is visibly apparent that σ_X has no rotational symmetry.

Figures 5(A) to 5(F) display the graphs of σ_{X_m} in the cases $m \neq 1$. For each such m, the graph of σ_{X_m} contains a scaled copy of σ_{X_1} by Theorem 2.2 and has m-fold dihedral symmetry by Theorem 3.1, since $(20485m, 4608) = m$. It is evident from the associated figures that m is maximal in each case, in the sense that σ_{X_m} having k-fold dihedral symmetry implies $k \leqslant m$.



(A) $n = 2\cdot 20485$ (B) $n = 3\cdot 20485$ (C) $n = 4\cdot 20485$

(D) $n = 6\cdot 20485$ (E) $n = 8\cdot 20485$ (F) $n = 12\cdot 20485$

FIGURE 5. Graphs of cyclic supercharacters σ_X of $\mathbb{Z}/n\mathbb{Z}$, where $X = \langle 4609\rangle 1$. One can produce dihedrally symmetric images containing the one in Figure 4(B), each rotated copy of which is colored differently.

4. Real and imaginary supercharacters

The images of some cyclic supercharacters are subsets of the real axis. Many others are subsets of the union of the real and imaginary axes. In this section, we establish sufficient conditions for each situation to occur and provide explicit evaluations in certain cases. Let σ_X be a cyclic supercharacter of $\mathbb{Z}/n\mathbb{Z}$, where $X = Ar$. If A contains -1, then it is immediate from (1) that σ_X is real-valued.

Example 4.1. Let X be the orbit of 3 under the action of $\langle 164 \rangle$ on $\mathbb{Z}/855\mathbb{Z}$. Since $164^3 \equiv -1 \pmod{n}$, it follows that σ_X is real-valued, as suggested by Figure 6(A).

Example 4.2. If $A = \langle -1 \rangle$ and $X = Ar$ where $r \neq \frac{n}{2}$, then $X = \{-r, r\}$ and $\sigma_X(y) = 2\cos(2\pi r y/n)$. Figure 6(B) illustrates this situation.

(A) $n = 855$, $A = \langle 164 \rangle$ (B) $n = 105$, $A = \langle 104 \rangle$ (C) $n = 121$, $A = \langle 94 \rangle$

Figure 6. Graphs of cyclic supercharacters σ_X of $\mathbb{Z}/n\mathbb{Z}$, where $X = A1$. Each σ_X is real-valued, since each A contains -1.

We turn our attention to cyclic supercharacters whose values, if not real, are purely imaginary (see Figure 7). To this end, we introduce the following notation. Let k be a positive divisor of n, and suppose that

$$A = \langle j_0 n/k - 1 \rangle, \quad \text{for some } 1 \leqslant j_0 < k. \tag{2}$$

In this situation, we have

$$(j_0 n/k - 1)^m \equiv (-1)^m \quad \left(\operatorname{mod} \tfrac{n}{k}\right),$$

so that every element of A has either the form $\frac{jn}{k} + 1$ or $\frac{jn}{k} - 1$, where $0 \leqslant j < k$. In this situation, we write

$$A = \{jn/k + 1 : j \in J_+\} \cup \{jn/k - 1 : j \in J_-\} \tag{3}$$

for some subsets J_+ and J_- of $\{0, 1, \ldots, k-1\}$.

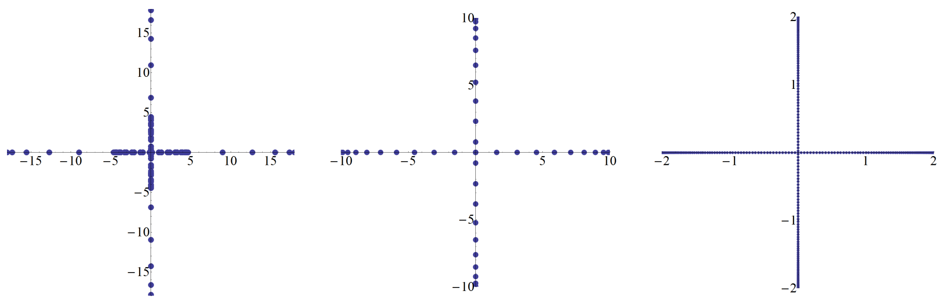
The condition (3) is vacuous if $k = n$. However, if $k < n$ and $j_0 > 1$ (i.e., if A is nontrivial), then it follows that $(-1)^{|A|} \equiv 1 \pmod{\frac{n}{k}}$, whence $|A|$ is even. In particular, this implies $|J_+| = |J_-|$. The subsets J_+ and J_- are not necessarily disjoint. For instance, if $A = \langle -1 \rangle = \{-1, 1\}$, then (3) holds where $k = 1$ and $J_+ = J_- = \{0\}$. In general, J_+ must contain 0, since A must contain 1. The following result is typical of those obtained by imposing restrictions on J_+ and J_-.

Proposition 4.3. *Let σ_X be a cyclic supercharacter of $\mathbb{Z}/n\mathbb{Z}$, where $X = Ar$, and suppose that (3) holds, where k is even and $J_- = \frac{k}{2} - J_+$.*

(i) *If r is even, then the image of σ_X is a subset of the real axis.*

(ii) *If r is odd, then $\sigma_X(y)$ is real whenever y is even and purely imaginary whenever y is odd.*

Proof. Each x in X has the form $(jn/k+1)r$ or $((k/2 - j)\, n/k + 1)\, r$. If $y = 2m$ for some integer m, then for every summand $e(xy/n)$ in the definition of $\sigma_X(y)$ having the form $e\left(2m(jn/k + 1)r/n\right)$, there is one of the form $e\left(2m(n/2 - jn/k + 1)r/n\right)$, its complex conjugate. From this we deduce that $\sigma_X(y)$ is real whenever y is even. If $y = 2m+1$, then for every summand of the form $e\left((2m+1)\left(jn/k + 1\right) r/n\right)$, there is one of the form $e\left((2m+1)(n/2 - jn/k+1)r/n\right)$. If r is odd, then the latter is the former reflected across the imaginary axis, in which case $\sigma_X(y)$ is purely imaginary. If r is even, then the latter is the conjugate of the former, whence $\sigma_X(y)$ is real. $\square$



(A) $n = 912,\ A = \langle 71\rangle$ (B) $n = 400,\ A = \langle 39\rangle$ (C) $n = 552,\ A = \langle 275\rangle$

FIGURE 7. Graphs of cyclic supercharacters $\sigma_X : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ whose values are either real or purely imaginary.

Example 4.4. In the case of Figure 7(A), we have $n = 912$, $r = 1$, $k = 38$, $j_0 = 3$,

$$J_+ = \{0,2,12,16,20,22,24,26,32\}, \quad \text{and} \quad J_- = \{3,7,17,19,25,31,33,35,37\},$$

so the hypotheses of Proposition 4.3(ii) hold.

An explicit evaluation of σ_X is available if $J_+ \cup J_- = \{0,1,\ldots,k-1\}$. The following result, presented without proof, treats this situation (see Figure 7(B)).

Proposition 4.5. *Suppose that $k > 2$ is even, and that (3) holds where J_+ is the set of all even residues modulo k and J_- is the set of all odd residues. If X is the orbit of a unit r under the action of A on $\mathbb{Z}/n\mathbb{Z}$, then*

$$\sigma_X(y) = \begin{cases} k\cos\frac{2\pi r y}{n} & \text{if } k|y, \\ ik\sin\frac{2\pi r y}{n} & \text{if } y \equiv \frac{k}{2} \pmod{k}, \\ 0 & \text{otherwise.} \end{cases}$$

5. ELLIPSES

Discretized ellipses appear frequently in the graphs of cyclic supercharacters. These, in turn, form primitive elements from which more complicated supercharacter plots emerge. In order to proceed, we recall the definition of a Gauss sum. Suppose that m and k are integers with $k > 0$. If χ is a Dirichlet character modulo k, then the *Gauss sum* associated with χ is given by

$$G(m,\chi) = \sum_{\ell=1}^{k} \chi(\ell) e\left(\frac{\ell m}{k}\right).$$

If p is prime, the *quadratic Gauss sum* $g(m;p)$ over $\mathbb{Z}/p\mathbb{Z}$ is given by $g(m;p) = g(m,\chi)$, where $\chi(a) = \left(\frac{a}{p}\right)$ is the Legendre symbol of a and p. That is,

$$g(m;p) = \sum_{\ell=0}^{k-1} e\left(\frac{m\ell^2}{p}\right).$$

We require the following well-known result [3, Thm. 1.5.2].

Lemma 5.1. *If $p \equiv 1 \pmod 4$ is prime and $(m,p) = 1$, then*

$$g(m;p) = \left(\frac{m}{p}\right)\sqrt{p}.$$

Proposition 5.2. *Suppose that $p|n$ and $p \equiv 1 \pmod 4$ is prime. Let*

$$Q_p = \{m \in \mathbb{Z}/p\mathbb{Z} : \left(\frac{m}{p}\right) = 1\}$$

denote the set of distinct nonzero quadratic residues modulo p. If (3) holds where

$$J_+ = \{aq + b : q \in Q_p\} \quad \text{and} \quad J_- = \{cq - b : q \in Q_p\} \tag{4}$$

for integers a, b, c coprime to p with $\left(\frac{a}{p}\right) = -\left(\frac{c}{p}\right)$, then $\sigma_X(y)$ belongs to the real interval $[1-p, p-1]$ whenever $p|y$, and otherwise belongs to the ellipse described by the equation $(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2/p = 1$.

Proof. For all y in $\mathbb{Z}/n\mathbb{Z}$, we have

$$\begin{aligned}
\sigma_X(y) &= \sum_{x \in A} e\left(\frac{xy}{n}\right) \\
&= \sum_{j \in J_+} e\left(\frac{\left(\frac{jn}{p} + 1\right) y}{n}\right) + \sum_{j \in J_-} e\left(\frac{(\frac{jn}{p} - 1)y}{n}\right) \\
&= \sum_{q \in Q_p} e\left(\frac{(aq+b)y}{p} + \frac{y}{n}\right) + \sum_{q \in Q_p} e\left(\frac{(cq-b)y}{p} - \frac{y}{n}\right) \\
&= e\left(\frac{by}{p} + \frac{y}{n}\right) \sum_{q \in Q_p} e\left(\frac{aqy}{p}\right) + e\left(-\frac{by}{p} - \frac{y}{n}\right) \sum_{q \in Q_p} e\left(\frac{cqy}{p}\right) \\
&= e(\theta_y) \sum_{\ell=1}^{(p-1)/2} e\left(\frac{a\ell^2 y}{p}\right) + \overline{e(\theta_y)} \sum_{\ell=1}^{(p-1)/2} e\left(\frac{c\ell^2 y}{p}\right),
\end{aligned}$$

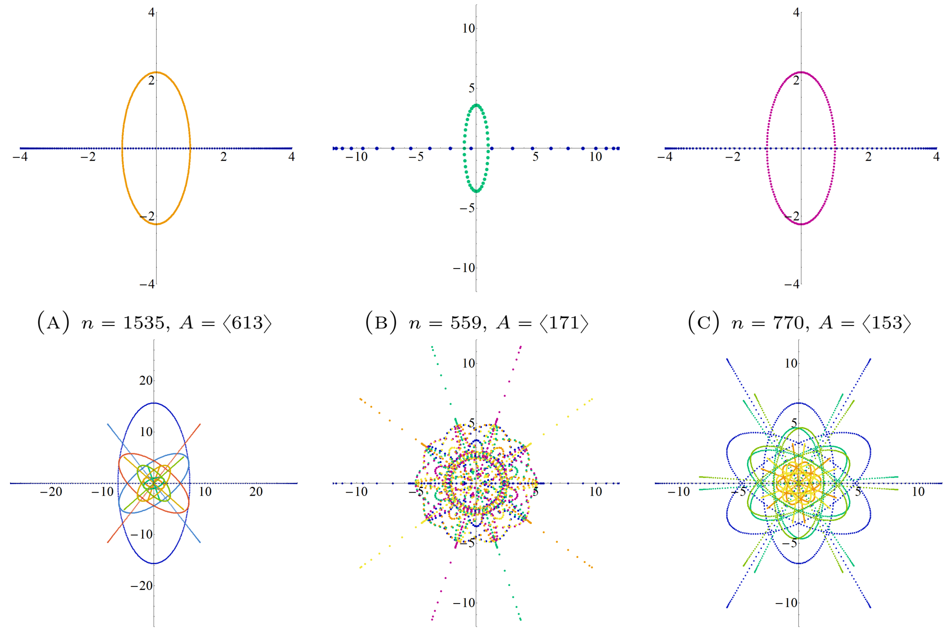
where $\theta_y = \frac{(bn+p)y}{pn}$. If $p|y$, then $e(\theta_y) = e(\frac{y}{n})$ and $e(\frac{a\ell^2 y}{p}) = e(\frac{c\ell^2 y}{p}) = 1$, so

$$\sigma_X(y) = \frac{(p-1)}{2}\left(e\left(\frac{y}{n}\right) + \overline{e\left(\frac{y}{n}\right)}\right) = (p-1)\cos\frac{2\pi y}{n}.$$

If not, then $(p, y) = 1$ so that Lemma 5.1 yields

$$\begin{aligned}
\sigma_X(y) &= \frac{e(\theta_y)\left(g(ay;p) - 1\right) + \overline{e(\theta_y)}(g(cy;p) - 1)}{2} \\
&= \frac{e(\theta_y) g(ay;p) + \overline{e(\theta_y)} g(cy;p)}{2} - \cos 2\pi\theta_y \\
&= \frac{\sqrt{p}}{2}\left(\left(\frac{ay}{p}\right) e(\theta_y) + \left(\frac{cy}{p}\right)\overline{e(\theta_y)}\right) - \cos 2\pi\theta_y \\
&= \pm\left(\frac{y}{p}\right)\frac{\sqrt{p}}{2}\left(e(\theta_y) - \overline{e(\theta_y)}\right) - \cos 2\pi\theta_y \\
&= \pm i\left(\frac{y}{p}\right)\sqrt{p}\sin 2\pi\theta_y - \cos 2\pi\theta_y,
\end{aligned}$$

□



(A) $n = 1535,\ A = \langle 613 \rangle$ (B) $n = 559,\ A = \langle 171 \rangle$ (C) $n = 770,\ A = \langle 153 \rangle$

(D) $n = 1535 \cdot 43,\ A = \langle 613 \rangle$ (E) $n = 559 \cdot 7 \cdot 5,\ A = \langle 171 \rangle$ (F) $n = 770 \cdot 13 \cdot 3,\ A = \langle 1693 \rangle$

FIGURE 8. Graphs of cyclic supercharacters σ_X of $\mathbb{Z}/n\mathbb{Z}$, where $X = A1$. Propositions 2.2, 3.1 and 5.2 can be used to produce supercharacters whose images feature elliptical patterns.

Example 5.3. Let $n = d = 1088 = 4^3 \cdot 17$ and consider the orbit X of $r = 1$ under the action of $A = \langle 63 \rangle = \langle \frac{n}{17} - 1 \rangle$ on $\mathbb{Z}/n\mathbb{Z}$. In this situation, illustrated by Figure 8(A), (3) holds with $J_+ = \{0, 4\} = 2Q_5 + 2$ and $J_- = \{2, 4\} = Q_{17} + 3$. Figure 8(B) illustrates the situation $J_+ = Q_{13} + 3$ and $J_- = 2Q_{13} - 3$, while Figure 8(C) illustrates $J_+ = Q_5 + 1$ and $J_- = 2Q_2 - 1$. The remainder of Figure 8 demonstrates the effect of using Propositions 2.2, 3.1 and 5.2 to produce supercharacters whose images feature ellipses.

6. Asymptotic behavior

We now turn our attention to an entirely different matter, namely the asymptotic behavior of cyclic supercharacter plots. To this end we begin by recalling several definitions and results concerning uniform distribution modulo 1. The *discrepency* of a finite subset S of $[0, 1)^m$ is the quantity

$$D(S) = \sup_{B} \left| \frac{|B \cap S|}{|S|} - \mu(B) \right|,$$

where the supremum runs over all boxes $B = [a_1, b_1) \times \cdots \times [a_m, b_m)$ and μ denotes m-dimensional Lebesgue measure. We say that a sequence S_n of finite subsets of $[0, 1)^d$ is *uniformly distributed* if $\lim_{n\to\infty} D(S_n) = 0$. If S_n is a sequence of finite subsets in $\mathbb{R}^m$, we say that S_n is *uniformly distributed mod* 1 if the corresponding sequence of sets $\big\{(\{x_1\}, \{x_2\}, \ldots, \{x_d\}) : (x_1, x_2, \ldots, x_m) \in S_n\big\}$ is uniformly distributed in $[0, 1)^m$. Here $\{x\}$ denotes the fractional part $x - \lfloor x \rfloor$ of a real number x. The following fundamental result is due to H. Weyl [13].

Lemma 6.1. *A sequence of finite sets S_n in $\mathbb{R}^m$ is uniformly distributed modulo 1 if and only if*

$$\lim_{n\to\infty} \frac{1}{|S_n|} \sum_{\mathbf{u}\in S_n} e(\mathbf{u}\cdot\mathbf{v}) = 0$$

for each $\mathbf{v}$ in $\mathbb{Z}^m$.

In the following, we suppose that $q = p^a$ is a nonzero power of an odd prime and that $|X| = d$ is a divisor of $p-1$. Let ω_q denote a primitive dth root of unity modulo q and let

$$S_q = \left\{ \frac{\ell}{q}(1, \omega_q, \omega_q^2, \ldots, \omega_q^{\varphi(d)-1}) : \ell = 0, 1, \ldots, q-1 \right\} \subseteq [0,1)^{\varphi(d)}$$

where φ denotes the Euler totient function. The following lemma of Myerson, whose proof we have adapted to suit our notation, can be found in [11, Thm. 12].

Lemma 6.2. *The sets S_q for $q \equiv 1 \pmod d$ are uniformly distributed modulo 1.*

Proof. Fix a nonzero vector $\mathbf{v} = (a_0, a_1, \ldots, a_{\varphi(d)-1})$ in $\mathbb{Z}^{\varphi(d)}$ and let

$$f(t) = a_0 + a_1 t + \cdots + a_{\varphi(d)-1} t^{\varphi(d)-1}.$$

Let $r = q/(q, f(\omega_q))$, and observe that

$$\begin{aligned}
\sum_{\mathbf{u}\in S_q} e(\mathbf{u}\cdot\mathbf{v}) &= \sum_{\ell=0}^{q-1} e\left(\frac{f(\omega_q)\ell}{q}\right) \\
&= \sum_{m=0}^{q/r-1} \sum_{\ell=mr}^{(m+1)r-1} e\left(\frac{f(\omega_q)\ell}{r}\right) \\
&= \frac{q}{r} \sum_{\ell=0}^{r-1} e\left(\frac{f(\omega_q)\ell}{r}\right) \\
&= \begin{cases} q & \text{if } q | f(\omega_q), \\ 0 & \text{else.} \end{cases}
\end{aligned}$$

Having fixed d and $\mathbf{v}$, we claim that the sum above is nonzero for only finitely many $q \equiv 1 \pmod d$. Letting Φ_d denote the dth cyclotomic polynomial, recall that $\deg \Phi_d = \varphi(d)$ and that Φ_d is the minimal polynomial of any primitive dth root of unity. Clearly the gcd of $f(t)$ and $\Phi_d(t)$ as polynomials in $\mathbb{Q}[t]$ is in $\mathbb{Z}$. Thus there exist $a(t)$ and $b(t)$ in $\mathbb{Z}[t]$ so that $a(t)\Phi_d(t) + b(t)f(t) = n$ for some integer n. Passing to $\mathbb{Z}/q\mathbb{Z}$ and letting $t = \omega_q$, we find that $b(\omega_q)f(\omega_q) \equiv n \pmod p$. This means that $q | f(\omega_q)$ implies that $q|n$, which can occur for only finitely many prime powers q. Putting this all together, we find that

$$\lim_{\substack{q\to\infty \\ q\equiv 1 \pmod d}} \frac{1}{|S_q|} \sum_{\mathbf{u}\in S_q} e(\mathbf{u}\cdot\mathbf{v}) = 0$$

holds for all $\mathbf{v}$ in $\mathbb{Z}^{\varphi(d)}$. By Weyl's Criterion, it follows that the sets S_q are uniformly distributed mod 1 as $q \equiv 1 \pmod d$ tends to infinity. □

Theorem 6.3. *Let σ_X be a cyclic supercharacter of $\mathbb{Z}/q\mathbb{Z}$, where $q = p^a$ is a nonzero power of an odd prime. If $X = A1$ and $|X| = d$ divides $p-1$, then the image of σ_X is contained in the image of the function $g : [0,1)^{\varphi(d)} \to \mathbb{C}$ defined by*

$$g(z_1, z_2, \ldots, z_{\varphi(d)}) = \sum_{k=0}^{d-1} \prod_{j=0}^{\varphi(d)-1} z_{j+1}^{b_{k,j}} \tag{5}$$

where the integers $b_{k,j}$ are given by

$$t^k \equiv \sum_{j=0}^{\varphi(d)-1} b_{k,j} t^j \pmod{\Phi_d(t)}. \tag{6}$$

For a fixed d, as q becomes large, the image of σ_X fills out the image of g, in the sense that, given $\epsilon > 0$, there exists some $q \equiv 1 \pmod d$ such that if $\sigma_X : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ is a cyclic supercharacter with $|X| = d$, then every open ball of radius $\epsilon > 0$ in the image of g has nonempty intersection with the image of σ_X.

Proof. Let ω_q be a primitive dth root of unity modulo q, so that $A = \langle \omega_q \rangle$ in $(\mathbb{Z}/q\mathbb{Z})^\times$. Recall that $\{1, e(\frac{1}{d}), \ldots, e(\frac{\varphi(d)-1}{d})\}$ is a $\mathbb{Z}$-basis for the ring of integers of the cyclotomic field $\mathbb{Q}(e(\frac{1}{d}))$ [12, Prop. 10.2]. For $k = 0, 1, \ldots, d-1$, the integers $b_{k,j}$ in the expression

$$e\left(\frac{k}{d}\right) = \sum_{j=0}^{\varphi(d)-1} b_{k,j} e\left(\frac{j}{d}\right),$$

are determined by (6). In particular, it follows that

$$\omega_p^k \equiv \sum_{j=0}^{\varphi(d)-1} b_{k,j} \omega_p^j \pmod p.$$

We have

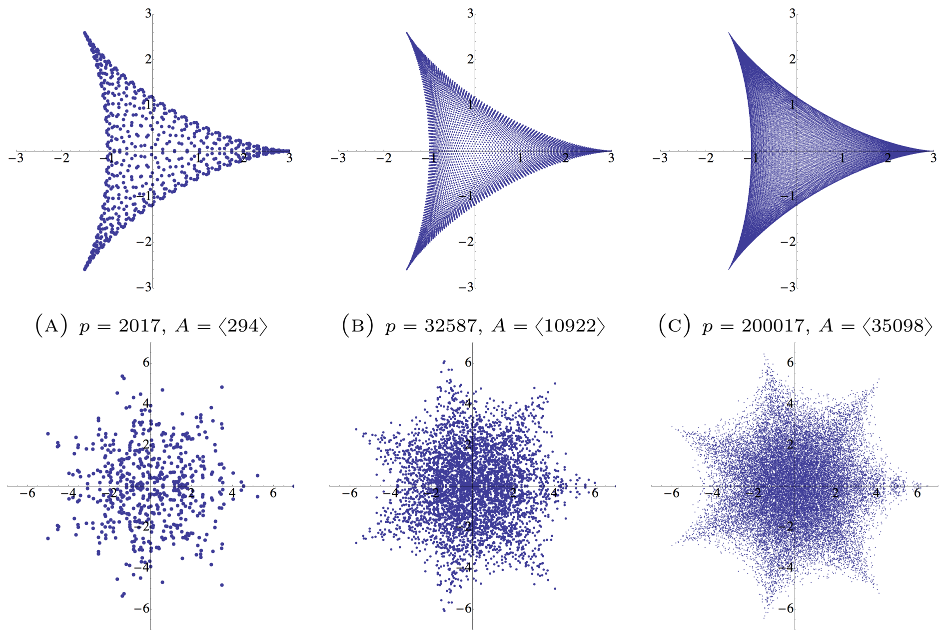
$$\sigma_X(y) = \sum_{x \in X} e\left(\frac{xy}{q}\right) = \sum_{k=0}^{d-1} e\left(\frac{\omega_p^k}{p}\right) = \sum_{k=0}^{d-1} e\left(\sum_{j=0}^{\varphi(d)-1} b_{k,j} \frac{\omega_p^j \ell}{p}\right),$$

from which it follows that the image of σ_X is contained in the image of the function $g : \mathbb{T}^{\varphi(d)} \to \mathbb{C}$ defined by (5). The density claim now follows from Lemma 6.2. $\square$

In combination with Propositions 2.2 and 2.4, the preceding theorem characterizes the boundary curves of cyclic supercharacters with prime power moduli. If d is even, then X is closed under negation, so σ_X is real. If $d = p^a$ where p is an odd prime, then $g : \mathbb{T}^{\varphi(p^a)} \to \mathbb{C}$ is given by

$$g(z_1, z_2, \cdots, z_{\varphi(d)}) = \sum_{j=1}^{\varphi(d)} z_j + \sum_{j=1}^{p^{a-1}} \prod_{\ell=0}^{p-2} z_{j+\ell p^{a-1}}^{-1}.$$

A particularly concrete manifestation of our result is Theorem 1.1, whose proof we present below. Recall that a *hypocycloid* is a planar curve obtained by tracing the path of a distinguished point on a small circle which rolls within a larger circle. Rolling a circle of integral radius λ within a circle of integral radius κ, where $\kappa > \lambda$, yields the parametrization $\theta \mapsto (\kappa - \lambda)e^{i\theta} + \lambda e^{(1-\kappa/\lambda)i\theta}$ of the hypocycloid centered at the origin, containing the point κ, and having precisely κ cusps.



(A) $p = 2017,\ A = \langle 294 \rangle$ (B) $p = 32587,\ A = \langle 10922 \rangle$ (C) $p = 200017,\ A = \langle 35098 \rangle$

(D) $p = 4019,\ A = \langle 1551 \rangle$ (E) $p = 32173,\ A = \langle 3223 \rangle$ (F) $p = 200033,\ A = \langle 11073 \rangle$

FIGURE 9. Cyclic supercharacters σ_X of $\mathbb{Z}/p\mathbb{Z}$, where $X = A1$, whose graphs fill out $|X|$-hypocycloids.

Pf. of Thm. 1.1. Computing the coefficients $b_{k,j}$ from (6) we find that $b_{k,j} = \delta_{kj}$ for $k = 0, 1, \ldots, d-2$, and $b_{d-1,j} = -1$ for all j, from which (5) yields

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

The image of the function $g : \mathbb{T}^{d-1} \to \mathbb{C}$ defined above is the filled hypocycloid corresponding to the parameters $\kappa = d$ and $\lambda = 1$, as observed in [9, §3]. □

References

[1] Carlos A. M. André. The basic character table of the unitriangular group. *J. Algebra*, 241(1):437–471, 2001.

[2] Carlos A. M. André. Basic characters of the unitriangular group (for arbitrary primes). *Proc. Amer. Math. Soc.*, 130(7):1943–1954 (electronic), 2002.

[3] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons Inc., New York, 1998. A Wiley-Interscience Publication.

[4] J.L. Brumbaugh, Madeleine Bulkow, Patrick S. Fleming, Luis Alberto Garcia, Stephan Ramon Garcia, Gizem Karaali, Matthew Michal, and Andrew P. Turner. Supercharacters, exponential sums, and the uncertainty principle. (preprint) `http://arxiv.org/abs/1208.5271`.

[5] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000.

[6] Persi Diaconis and I. M. Isaacs. Supercharacters and superclasses for algebra groups. *Trans. Amer. Math. Soc.*, 360(5):2359–2392, 2008.

[7] P.S. Fleming, S.R. Garcia, and G. Karaali. Classical Kloosterman sums: representation theory, magic squares, and Ramanujan multigraphs. *J. Number Theory*, 131(4):661–680, 2011.

[8] Christopher Fowler, Stephan Ramon Garcia, and Gizem Karaali. Ramanujan sums as supercharacters. *Ramanujan J.* (in press) `http://arxiv.org/abs/1201.1060`.
[9] N. Kaiser. Mean eigenvalues for simple, simply connected, compact Lie groups. *J. Phys. A*, 39(49):15287–15298, 2006.
[10] D. H. Lehmer and Emma Lehmer. Cyclotomy with short periods. *Math. Comp.*, 41(164):743–758, 1983.
[11] Gerald Myerson. A combinatorial problem in finite fields. II. *Quart. J. Math. Oxford Ser. (2)*, 31(122):219–231, 1980.
[12] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
[13] H. Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, 77(3):313–352, 1916.

Department of Mathematics, UCLA, Los Angeles, California, 90095-1555, USA
E-mail address: `wdduke@ucla.edu`
URL: `http://www.math.ucla.edu/~wdduke/`

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

Current address: Department of Mathematics, University of Michigan, 2074 East Hall, 530 Church Street, Ann Arbor, MI 48109-1043
E-mail address: `boblutz@umich.edu`