THE GRAPHIC NATURE OF GAUSSIAN PERIODS

WILLIAM DUKE, STEPHAN RAMON GARCIA, AND BOB LUTZ

(Communicated by Ken Ono)

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 $\text{Irr}(G)$ 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

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

is constant on each $K \in \mathcal{K}$. The functions $\sigma_X$ 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 $\chi_x(y) = e\left(\frac{xy}{n}\right)$ 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

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

Received by the editors July 26, 2013.


The first author was partially supported by National Science Foundation Grants DMS-10-01527, DMS-1001614, and DMS-1265973.

©2015 American Mathematical Society
Reverts to public domain 28 years from publication.
where $X$ is an orbit in $\mathbb{Z}/n\mathbb{Z}$ under the action of $A$. When $n = p$ is an odd prime, (11) is a Gaussian period, a central object in the theory of cyclotomy. For $p = kd + 1$, Gauss defined the $d$-nomial periods $\eta_j = \sum_{\ell=0}^{d-1} \zeta_p^{k\ell+j}$, where $\zeta_p = e^{(1/p)}$ and $g$ denotes a primitive root modulo $p$ [35]. Clearly $\eta_j$ runs over the same values as $\sigma_X(y)$ when $y \neq 0$, $|A| = d$, and $X = A1$ is the $A$-orbit of 1. For composite moduli, the functions $\sigma_X$ attain values which are generalizations of Gaussian periods of the type considered by Kummer and others (see [10]).

![Image](image1)

**Figure 1.** Each subfigure is the image of $\sigma_X : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C}$, 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 $y \neq y' \pmod{m}$, 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
Table 1. Gaussian periods, Ramanujan sums, Kloosterman sums, and Heilbronn sums appear as supercharacters arising from the action of a subgroup $A$ of $\text{Aut } G$ for a suitable abelian group $G$. Here $p$ denotes an odd prime number.

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

attention on the case where $A = \langle \omega \rangle$ is a cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. We refer to supercharacters 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.

**Theorem 1.1.** Suppose that $q = p^a$ is an odd prime power and that $\sigma_X$ is a cyclic supercharacter of $\mathbb{Z}/q\mathbb{Z}$. If $|X| = d$ is prime and $d \neq p$, then the image of $\sigma_X$ 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 $q = 1 \pmod{d}$ 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).

![Figure 2](image-url)  
**Figure 2.** Graphs of cyclic supercharacters $\sigma_X : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ where $X = A1$. 

(A) $p = 2791$, $A = (869)$  
(B) $p = 27011$, $A = (2699)$  
(C) $p = 202231$, $A = (61576)$
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 $(\mathbb{Z}/n\mathbb{Z})^\times$. The following is a simple consequence of the Chinese Remainder Theorem.

Theorem 2.1. Suppose that $\sigma_{(\omega, r)}$ is a cyclic supercharacter on $\mathbb{Z}/mn\mathbb{Z}$, where $(m, n) = 1$, and let $\rho : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ be the natural isomorphism. If $\rho(\omega) = (\omega_m, \omega_n)$, $\rho(r) = (r_m, r_n)$, and $a, b \in \mathbb{Z}$ with $mb + na = 1$, then for all $y \in \mathbb{Z}/mn\mathbb{Z}$ we have

$$\sigma_{(\omega, r)}(y) = \sigma_{(\omega_m, r_m)}(ay)\sigma_{(\omega_n, r_n)}(by).$$

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 $r \in \mathbb{Z}/n\mathbb{Z}$, and suppose that $(r, n) = \frac{n}{d}$ for some positive divisor $d$ of $n$, so that $\xi = \frac{r d}{n}$ is a unit modulo $n$. Also let $\psi_d : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ be reduction modulo $d$.

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

(ii) The images of $\sigma_{\psi_d(A)1}$ and $\sigma_{A\xi}$ are equal.

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

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 $\sigma_X$, 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).

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 $\psi$ the natural homomorphism from $\mathbb{Z}/p^a\mathbb{Z}$ to $\mathbb{Z}/p^{a-b}\mathbb{Z}$. If $\sigma_X$ is a cyclic supercharacter of $\mathbb{Z}/p^{a-b}\mathbb{Z}$, where $X = A1$ with $p^b||X|$ and $p^{a-b} = 1 \pmod {||\psi(X)||}$, then

$$\sigma_X(\mathbb{Z}/p^a\mathbb{Z}) = \{0\} \cup p^b\sigma_{\psi(X)}(\mathbb{Z}/p^{a-b}\mathbb{Z}).$$
Figure 3. Graphs of cyclic supercharacters $\sigma_X$ 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.

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., $X' = \psi(X)$), so that

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

We have

$$\sigma_X(y) = \sum_{x \in X'} \sum_{j=0}^{p^b-1} e \left( \frac{(x + jp^{a-b})y}{p^a} \right)$$

$$= \sum_{j=0}^{p^b-1} e \left( \frac{y}{p^b} \right) \sum_{x \in X'} e \left( \frac{xy}{p^a} \right)$$

$$= \begin{cases} p^b \sigma_{X'}(\psi(y)), & \text{if } p^b | y \\ 0, & \text{else.} \end{cases}$$
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, $\sigma_X$ 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 $\sigma_X$ is generally asymmetric about the imaginary axis, as evidenced by Figure 4.

![Graphs](image)

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

**Proof.** Let $d = n/(r, n)$. If $k = (\omega - 1, d)$, then $\omega$, and hence every element of $\langle \omega \rangle$, has the form $jk + 1$. Since $r = \xi n/d$ for some unit $\xi$, 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

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

where $n = \prod p_i^{e_i}$ is the prime factorization of $n$. The conclusion follows from the fact that $(\omega - 1, d)$ must divide $\frac{n}{(r, n)}$. 


whence
\[
\xi_n \frac{(jk + 1)y'}{d} = \xi_n \frac{(jk + 1)y + \xi_n}{k} (j k + 1) (\text{mod } n)
\]
\[
= \xi_n \frac{(jk + 1)y + \xi_n}{k} (\text{mod } n).
\]
Since the function \( e \) is periodic with period 1, we have
\[
\sum_{x \in X} e \left( \frac{xy'}{n} \right) = \sum_{x \in X} e \left( \frac{xy + \xi_n}{n} \right) = e \left( \frac{\xi}{k} \right) \sum_{x \in X} e \left( \frac{xy}{n} \right).
\]
In other words, the image of \( \sigma_X \) 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 image of \( \sigma_X \) contains both \( \sigma_X(y) \) and \( \sigma_X(y) = \sigma_X(-y) \).

\[\square\]

**Figure 5.** Graphs of cyclic supercharacters \( \sigma_X \) of \( \mathbb{Z}/n\mathbb{Z} \), where \( X = \langle 4609 \rangle 1 \). One can produce dihedrally symmetric images containing the one in Figure 3(B), each rotated copy of which is colored differently.

**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 \( \sigma_{X_1} \), whose graph appears in Figure 3(B). We have \( (20485, 4608) = (5 \cdot 17 \cdot 241, 2^9 \cdot 3^2) = 1 \), so Proposition 3.1 guarantees that \( \sigma_{X_1} \) has 1-fold dihedral symmetry. It is visibly apparent that \( \sigma_X \) has no rotational symmetry.

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

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 $\sigma_X$ be a cyclic supercharacter of $\mathbb{Z}/n\mathbb{Z}$, where $X = Ar$. If $A$ contains $-1$, then it is immediate from (1) that $\sigma_X$ 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 $\sigma_X$ is real-valued, as suggested by Figure 6(A).

Example 4.2. If $A = \langle -1 \rangle$ and $X = Ar$ where $r \neq \frac{2}{3}$, then $X = \{-r, r\}$ and $\sigma_X(y) = 2\cos(2\pi ry/n)$. Figure 6(B) illustrates this situation.

![Figure 6](image)

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

![Figure 7](image)

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

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

$$A = \langle j_0n/k - 1 \rangle, \quad \text{for some } 1 \leq j_0 < k.$$  

(2)

In this situation, we write

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

(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 $(-1)^{|A|} \equiv 1 \pmod{\frac{n}{2}}$, whence $|A|$ is even. In particular, this implies $|J_+| = |J_-|$. The subsets $J_+$ and $J_-$ are not necessarily
disjoint. For instance, if \( A = \{-1,1\} \), 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 \( \sigma_X \) 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 \( \sigma_X \) 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 \((j/k - j)n/k + 1)r\). If \( y = 2m \) for some integer \( m \), then for every summand \( e(xy/n) \) in the definition of \( \sigma_X(y) \) having the form \( e((2m(n - j)n/k + 1)r/n) \), there is one of the form \( e((2m(n - j)n/k + 1)r/n) \) 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 \( e((2m + 1)(jn/k + 1)r/n) \), there is one of the form \( e((2m + 1)(n/k + 1)r/n) \). 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. \( \square \)

**Example 4.4.** In the case of Figure 7(A), we have \( n = 912 \), \( r = 1 \), \( k = 38 \), \( j_0 = 3 \), \( J_+ = \{0,2,12,16,20,22,24,32\} \), and \( J_- = \{3,7,17,19,25,31,33,35,37\} \), so the hypotheses of Proposition 4.3(ii) hold.

An explicit evaluation of \( \sigma_X \) 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

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

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 \( \chi \) is a Dirichlet character modulo \( k \), then the **Gauss sum** associated with \( \chi \) 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
\[
g(m; p) = \left( \frac{m^2}{p} \right) \sqrt{p}.
\]

Proposition 5.2. Suppose that \( p|n \) and \( p \equiv 1 \pmod{4} \) is prime. If (3) holds where
\[
J_+ = \{ \alpha \ell^2 + b : \ell = 1, 2, \ldots, \frac{p-1}{2} \}
\]
and \( J_- = \{ \chi \ell^2 - b : x = 1, 2, \ldots, \frac{p-1}{2} \} \)
for \( a, b, c \in \mathbb{Z} \) 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 \((\Re z)^2 + (\Im z)^2/p = 1\).

Proof. For all \( y \in \mathbb{Z}/n\mathbb{Z} \), we have
\[
\sigma_X(y) = \sum_{x \in A} e\left( \frac{xy}{n} \right)
= \sum_{j \in J_+} e\left( \frac{(jn + 1)y}{n} \right) + \sum_{j \in J_-} e\left( \frac{(jn - 1)y}{n} \right)
= \sum_{\ell=1}^{(p-1)/2} e\left( \frac{(\alpha \ell^2 + b)y}{p} + \frac{y}{n} \right) + \sum_{\ell=1}^{(p-1)/2} e\left( \frac{c \ell^2 - b - y}{p} \right)
= e\left( \frac{by}{p} + \frac{y}{n} \right) \sum_{\ell=1}^{(p-1)/2} e\left( \frac{a \ell^2 y}{p} \right) + e\left( -\frac{by}{p} - \frac{y}{n} \right) \sum_{\ell=1}^{(p-1)/2} e\left( \frac{c \ell^2 y}{p} \right)
= e(\theta y) \sum_{\ell=1}^{(p-1)/2} e\left( \frac{a \ell^2 y}{p} \right) + e(\theta y) \sum_{\ell=1}^{(p-1)/2} e\left( \frac{c \ell^2 y}{p} \right),
\]
where \( \theta = \frac{(bn+p)y}{pm} \). If \( p|y \), then \( e(\theta y) = e\left( \frac{y}{n} \right) \) and \( e\left( \frac{a \ell^2 y}{p} \right) = e\left( \frac{c \ell^2 y}{p} \right) = 1 \), so
\[
\sigma_X(y) = \frac{(p-1)}{2} \left( e\left( \frac{y}{n} \right) + e\left( \frac{y}{n} \right) \right) = (p-1) \cos \frac{2\pi y}{n}.
\]

If not, then \((p, y) = 1\), so
\[
\sigma_X(y) = \frac{e(\theta y) (g(ay; p) - 1) + e(\theta y) (g(cy; p) - 1)}{2}
= \frac{e(\theta y) g(ay; p) + e(\theta y) g(cy; p)}{2} - \cos 2\pi \theta y
= \frac{\sqrt{p}}{2} \left( e(\theta y) + e(\theta y) \right) - \cos 2\pi \theta y
= \pm \frac{\sqrt{p}}{2} \left( e(\theta y) - e(\theta y) \right) - \cos 2\pi \theta y
= \pm i \frac{\sqrt{p}}{2} \sin 2\pi \theta y - \cos 2\pi \theta y,
\]
where (5) follows from Lemma 5.1. \( \square \)

Example 5.3. Let \( n = 1535 = 5 \cdot 307 \) and consider the cyclic supercharacter \( \sigma_{(613)} \) on \( \mathbb{Z}/n\mathbb{Z} \). In this situation, illustrated by Figure 8(A), the hypotheses of Proposition 5.2 hold with \((a, b, c) = (2, 2, 1)\). Figure 8(B) illustrates the situation
Figure 8. Graphs of cyclic supercharacters $\sigma_X$ 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.

(a, b, c) = (1, 3, 2), while Figure 8(C) illustrates (1, 1, 2). 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 discrepancy 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 $\mu$ 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 $\left\{ \{(x_1), (x_2), \ldots, (x_d)\} : (x_1, x_2, \ldots, x_d) \in S_n \right\}$ is uniformly distributed in $[0, 1)^m$. Here $\{x\}$ denotes the fractional part $x - [x]$ 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

$$\lim_{n \to \infty} \frac{1}{|S_n|} \sum_{u \in S_n} e(u \cdot v) = 0$$
Theorem 6.3. Let \( q = p^a \) be a nonzero power of an odd prime and that \( |X| = d \) is a divisor of \( p - 1 \). Let \( \omega_q \) denote a primitive \( d \)th 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 \( \varphi \) 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 \( v = (a_0, a_1, \ldots, a_{\varphi(d)-1}) \) 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

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

Having fixed \( d \) and \( v \), we claim that the sum above is nonzero for only finitely many \( q \equiv 1 \pmod{d} \). Letting \( \Phi_d \) denote the \( d \)th cyclotomic polynomial, recall that \( \deg \Phi_d = \varphi(d) \) and that \( \Phi_d \) is the minimal polynomial of any primitive \( d \)th 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

\[
\lim_{q \to \infty} \frac{1}{|S_q|} \sum_{u \in S_q} e(u \cdot v) = 0
\]

holds for all \( v \) 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.

In what follows we let \( \mathbb{T} \) denote the unit circle in the complex plane.

Theorem 6.3. Let \( \sigma_X \) be a cyclic supercharacter of \( \mathbb{Z}/q\mathbb{Z} \), where \( q = p^a \) is a nonzero power of an odd prime. If \( X = A_1 \) and \( |X| = d \) divides \( p - 1 \), then the image of \( \sigma_X \) is contained in the image of the function \( g : \mathbb{T}^{\varphi(d)} \to \mathbb{C} \) defined by

\[
g(z_1, z_2, \ldots, z_{\varphi(d)}) = \sum_{k=0}^{d-1} \varphi(d)-1 \prod_{j=0}^{b_k} z_{j+1}^{b_k}
\]
where the integers $b_{k,j}$ are given by

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

For a fixed $d$, as $q$ becomes large, the image of $\sigma_X$ 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 $\sigma_X$.

Proof. Let $\omega_q$ be a primitive $d$th 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 $\mathbb{Q}(\zeta_d^\ell)$ [12 Prop. 10.2]. For $k = 0, 1, \ldots, d-1$, the integers $b_{k,j}$ in the expression

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

are determined by (7). In particular, it follows that

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

are determined by (7). In particular, it follows that

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

are determined by (7). 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

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

from which it follows that the image of $\sigma_X$ is contained in the image of the function $g : \mathbb{T}^\varphi(d) \to \mathbb{C}$ defined by (6). The density claim now follows from Lemma 6.2. □

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 $\sigma_X$ 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

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

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 $\lambda$ within a circle of integral radius $\kappa$, 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 $\kappa$, and having precisely $\kappa$ cusps.

Proof of Theorem 1.1 Computing the coefficients $b_{k,j}$ from (7) 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]. □
Figure 9. Cyclic supercharacters $\sigma_X$ of $\mathbb{Z}/p\mathbb{Z}$, where $X = A_1$, whose graphs fill out $|X|$-hypocycloids.

ACKNOWLEDGMENTS

Special thanks to Trevor Hyde for many helpful comments.

REFERENCES


Department of Mathematics, University of California, Los Angeles, Los Angeles, California 90095-1555

E-mail address: wdduke@ucla.edu
URL: http://www.math.ucla.edu/~wdduke/

Department of Mathematics, Pomona College, Claremont, California 91711

E-mail address: Stephan.Garcia@pomona.edu
URL: http://pages.pomona.edu/~sg064747

Department of Mathematics, University of Michigan, 2074 East Hall, 530 Church Street, Ann Arbor, Michigan 48109-1043

E-mail address: boblutz@umich.edu
URL: http://www-personal.umich.edu/~boblutz