1-1-2013

The Graphic Nature of Gaussian Periods

William Duke

Stephan Ramon Garcia  
\textit{Pomona College}

Bob Lutz ’13  
\textit{Pomona College}

Recommended Citation
http://scholarship.claremont.edu/pomona_fac_pub/232

This Article - preprint is brought to you for free and open access by the Pomona Faculty Scholarship at Scholarship @ Claremont. It has been accepted for inclusion in Pomona Faculty Publications and Research by an authorized administrator of Scholarship @ Claremont. For more information, please contact scholarship@cuc.claremont.edu.
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 with which to study the properties of 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, this approach reveals that these classical objects display a dazzling array of 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 [7], extending the seminal work of C. André [1–3]. Recent work has shown that the study of supercharacters on abelian groups provides a natural framework with which to study the properties of certain exponential sums of interest in number theory [5,9] (see also [8]). In particular, Gaussian periods, Ramanujan sums, Kloosterman sums, and Heilbronn sums can be realized in this way (see 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 \( \text{Irr}_p G \) of irreducible characters of \( G \). The ordered pair \( (\mathcal{X}, \mathcal{K}) \) is called a supercharacter theory for \( G \) if \( t_0 \in \mathcal{K}, |\mathcal{X}| \leq |\mathcal{K}| \), and for each \( \chi \in \mathcal{X} \), the (generalized) character

\[ \sigma_X = \sum_{\chi \in \mathcal{X}} \chi(0) \chi \]

is constant on each \( K \in \mathcal{K} \). The characters \( \sigma_X \) 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 \( (\mathbb{Z}/n\mathbb{Z})^* \), let \( \mathcal{K} \) denote the partition of \( \mathbb{Z}/n\mathbb{Z} \) arising from the action \( a \cdot x = ax \) of \( A \). Similarly, 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

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

where \( X \) is an orbit in \( \mathbb{Z}/n\mathbb{Z} \) under the action of a subgroup \( A \) of \( (\mathbb{Z}/n\mathbb{Z})^* \). 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 \( \eta_j = \sum_{k=0}^{d-1} c^k \ell^{kd+j} \),

Partially supported by National Science Foundation Grant DMS-1001614.
where \( \zeta_p = \exp(2\pi i/p) \) and \( g \) denotes a primitive root modulo \( p \). Clearly \( \eta_j \) runs over the same values as \( \sigma_X(y) \) when \( y \neq 0 \), \(|A| = d\), and \( X = A \) 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 [11]).

\[
\begin{align*}
(A) \ n &= 52059, \ A = \langle 766 \rangle \\
(B) \ n &= 91205, \ A = \langle 2337 \rangle \\
(C) \ n &= 70091, \ A = \langle 3447 \rangle \\
(D) \ n &= 91205, \ A = \langle 39626 \rangle \\
(E) \ n &= 91205, \ A = \langle 1322 \rangle \\
(F) \ n &= 95095, \ A = \langle 626 \rangle \\
(G) \ n &= 82677, \ A = \langle 8147 \rangle \\
(H) \ n &= 70091, \ A = \langle 21792 \rangle \\
(I) \ n &= 51319, \ A = \langle 430 \rangle
\end{align*}
\]

**Figure 1.** Each subfigure is the image of \( \sigma_X : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C} \) where \( X \) is the orbit of \( r = 1 \) under the action of \( A \leq (\mathbb{Z}/n\mathbb{Z})^\times \) on \( \mathbb{Z}/n\mathbb{Z} \).

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 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 $p$ is an odd prime and that $\sigma_X$ is a cyclic supercharacter on $\mathbb{Z}/p\mathbb{Z}$. If $|X| = d$ is prime, 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 $d$, as the modulus $p \equiv 1 \pmod{d}$ tends to infinity the corresponding supercharacter images become dense in the filled hypocycloid in a sense that will be made precise in Section 6.

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

**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.

The preceding theorem is itself a special case of a more general theorem (Theorem 6.3) which relates the asymptotic behavior of cyclic supercharacter plots to

![Graphs of cyclic supercharacters](image)

(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 $\sigma_X$ of $\mathbb{Z}/p\mathbb{Z}$, where $X = A1$, showing the density of hypocycloids as $p \to \infty$. 

The preceding theorem is itself a special case of a 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 a suitable, high-dimensional torus.

2. Nesting plots

Our first order of business is determining when the image of one cyclic supercharacter plot is contained in another. Following the introduction, we let \( X = \mathbb{A} \) denote the orbit of an element \( r \) of \( \mathbb{Z}/n\mathbb{Z} \) under the action of a cyclic subgroup \( A = \langle a \rangle \) of \( (\mathbb{Z}/n\mathbb{Z})^\times \). For each positive divisor \( d \) of \( n \), let \( \psi_d : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z} \) be the ring homomorphism that maps each element of \( \mathbb{Z}/n\mathbb{Z} \) to its residue modulo \( d \), so that \( \psi_d(A) = \langle \psi_d(a) \rangle \leq (\mathbb{Z}/d\mathbb{Z})^\times \) acts on \( \mathbb{Z}/d\mathbb{Z} \) by multiplication. As a consequence of the following result, we can observe all possible graphical behavior by restricting our attention to the case \( r = 1 \).

**Proposition 2.1.** Let \( r \) belong to \( \mathbb{Z}/n\mathbb{Z} \), and suppose that \( (r, n) = \frac{n}{r} \) for some positive divisor \( d \) of \( n \), so that \( \xi = \frac{r}{n} \) is a unit modulo \( n \).

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

(ii) The image in (i) is a scaled subset of the image of \( \sigma_{A\xi} \).

**Proof.** Label the supercharacters in the statement of the theorem in order of men-

1. Since \( c \xi n/d = c' \xi n/d \) (mod \( n \)) if and only if \( cn/d = c'n/d \) (mod \( n \)), we may assume that \( C_1 = C_2 \). For any \( y \) in \( \mathbb{Z}/n\mathbb{Z} \), letting \( y' = \xi^{-1}y \) gives

\[
\sigma_{X_1}(y') = \sum_{x \in X_1} e\left(\frac{xy'}{n}\right) = \sum_{c \in C_1} e\left(\frac{c\xi y'}{d}\right) = \sum_{c \in C_2} e\left(\frac{cy}{d}\right) = \sigma_{X_2}(y),
\]

so \( \text{im} \sigma_{X_2} \subset \text{im} \sigma_{X_1} \). Letting \( y' = \xi y \) instead gives \( \sigma_{X_2}(y'') = \sigma_{X_1}(y) \), proving the reverse containment. Since \( cn/d = c'n/d \) (mod \( n \)) if and only if \( c \equiv c' \) (mod \( d \)), we may assume that \( \psi_d(C_2) = C_3 \) and \( |C_2| = |C_3| \). We then have

\[
\sigma_{X_2}(y) = \sum_{c \in C_2} e\left(\frac{cy}{d}\right) = \sum_{c \in C_3} e\left(\frac{cy}{d}\right) = \sigma_{X_3} \circ \psi_d(y),
\]

since \( e \) is periodic with period 1. Hence \( \text{im} \sigma_{X_2} = \text{im} \sigma_{X_3} \), concluding the proof of (i). Since \( cr = c'r \) (mod \( n \)) if and only if \( c \xi = c' \xi \) (mod \( d \)), we may assume that \( C_1 = \psi_d(C_4) \). For any \( y \) in \( \mathbb{Z}/n\mathbb{Z} \), letting \( y' = \gamma n/d \) gives

\[
\sigma_{X_4}(y') = \sum_{c \in C_4} e\left(\frac{cy}{d}\right) = \frac{|C_4|}{|\psi_d(C_4)|} \sum_{c \in \psi_d(C_4)} e\left(\frac{cy}{d}\right) = \frac{|A|}{|\psi_d(A)|} \sigma_{X_4}(y),
\]

which concludes the proof of (ii). \( \square \)

**Example 2.2.** 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 \( \sigma_{X_i} \), where \( X \) is the orbit of \( \frac{n}{r} \) under the action of \( (319) \) on \( \mathbb{Z}/n\mathbb{Z} \) for some given positive divisor \( d \) of \( n \). By Proposition 2.1(i), each is equivalent to the image of \( \sigma_{X_i} \) where \( X_i \) is the orbit of 1 under the action of \( \psi_d((319)) = \langle \psi_d(319) \rangle \) on \( \mathbb{Z}/d\mathbb{Z} \). By Proposition 2.1(ii), each nests in Figure 3(\( \psi_d(319) \)).
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.

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

Proof. Let $d = n/(r, n)$. If $k = (u - 1, d)$, then the generator $u$, and hence every element of $\langle u \rangle$, has the form $jk + 1$. If $(r, n) = n/d$, then $r = \xi n/d$ where $(\xi, n) = 1$. Each $x$ in $X$ therefore has the form $(\xi n/d)(jk + 1)$. If $y' = y + d/k$, then $y' - y - d/k = 0 \pmod{n}$, 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

$$\frac{\xi n}{d}(jk + 1)y' = \frac{\xi n}{d}(jk + 1)y + \frac{\xi n}{k}(jk + 1) \pmod{n}.$$
Figure 4. Graphs of $\sigma_X$ of $\mathbb{Z}/n\mathbb{Z}$, where $X = Ar$, fixing $r = 1$. Odd values of $n/(r, n)$ can produce asymmetric images.

Example 3.2. For all $m = 1, 2, 3, 4, 6, 8, 12$, 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 4(B). We have $(20485, 4608) = (5 \cdot 17 \cdot 241, 2^9 \cdot 3^2) = 1$, so Theorem 3.1 guarantees that $\sigma_{X_1}$ has 1-fold dihedral symmetry. It is visibly apparent that $\sigma_X$ has only the trivial 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 $\sigma_X$, by Theorem 2.1 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 $\sigma_{X_m}$ having $k$-fold dihedral symmetry implies $k \leq m$. 
THE GRAPHIC NATURE OF GAUSSIAN PERIODS

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 \( r \neq \frac{n}{2} \), then \( X = \{-r, r\} \) and \( \sigma_X(y) = 2\cos(2\pi ry/n) \). Figure 6(B) illustrates this situation.

![Figure 6](image)

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
\[ A = \langle j_0 n/k - 1 \rangle, \quad \text{for some } 1 \leq j_0 < k. \] (2)

In this situation, we have
\[ (j_0 n/k - 1)^m \equiv (-1)^m \quad (\text{mod } \frac{k}{2}), \]
so that every element of $A$ has either the form $\frac{jn}{k} + 1$ or $\frac{jn}{k} - 1$, where $0 \leq j < k$.

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 $A = \langle -1 \rangle = \{-1, 1\}$, 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 obtainable by imposing restrictions on $J_+$ and $J_-$.\[ \text{Figure 7. Graphs of cyclic supercharacters } \sigma_X \text{ of } \mathbb{Z}/n\mathbb{Z}, \text{ where } X = A1. \text{ Some cyclic supercharacters have values that are either real or purely imaginary.} \]

**Proposition 4.3.** Let $\sigma_X$ be a cyclic supercharacter of $\mathbb{Z}/n\mathbb{Z}$, where $X = A1$, 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 $((k/2 - j)n/k + 1)r$. If $y = 2m$ for some integer $m$, then for every summand $e(xy/n)$ in the definition of $\sigma_X(y)$ having the form $e(2m(jn/k + 1)r/n)$, there is one of the form $e(2m(n/2 - jn/k + 1)r/n)$, 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 $e((2m + 1)(n/2 - jn/k + 1)r/n)$. 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 complex conjugate of the former, in which case $\sigma_X(y)$ is real. \qed
Example 4.4. In the case of Figure 7(a) we have $n = 912$, $r = 1$, $k = 38$, $j_0 = 3$, $J_+ = \{0, 2, 12, 16, 20, 22, 24, 26, 32\}$, 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 $J_0 \cup J_1 = \{0, 1, \ldots, k - 1\}$. 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 $J_0$ is the set of all even residues modulo $k$ and $J_1$ 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

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

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 $\chi$ 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 [4 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 $p \mid n$ 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 $J_+ = \{aq + b : q \in Q_p\}$ and $J_- = \{cq - b : q \in Q_p\}$ (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 $p \mid y$, and otherwise belongs to the ellipse described by the equation $(\text{Re } z)^2 + (\text{Im } z)^2 / p = 1$. 

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

$\sigma_X(y) = \sum_{x \in \mathcal{X}} e\left(\frac{xy}{n}\right) = \sum_{j \in \mathcal{J}_+} e\left(\frac{(jn+1)y}{n}\right) + \sum_{j \in \mathcal{J}_-} e\left(\frac{(jn-1)y}{n}\right) = \sum_{q \in \mathbb{Q}_p} e\left(\frac{(aq+b)y}{p} + \frac{y}{n}\right) + \sum_{q \in \mathbb{Q}_p} e\left(\frac{(cq-b)y - y}{n}\right) = e\left(\frac{by+y}{p}\right) \sum_{q \in \mathbb{Q}_p} e\left(\frac{aqy}{p}\right) + e\left(-\frac{by-y}{n}\right) \sum_{q \in \mathbb{Q}_p} e\left(\frac{cqu}{p}\right) = e(\theta_y) \sum_{\ell=1}^{(p-1)/2} e\left(\frac{\alpha_\ell^2y}{p}\right) + e(\bar{\theta}_y) \sum_{\ell=1}^{(p-1)/2} e\left(\frac{\bar{c}\ell^2y}{p}\right),$

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

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

If not, then $(p, y) = 1$, so

$\sigma_X(y) = e(\theta_y) \left[g(ay; p) - 1 + \overline{e(\theta_y)}g(cy; p) - 1\right] = e(\theta_y)g(ay; p) + \overline{e(\theta_y)}g(cy; p) - \cos 2\pi \theta_y$

$= \frac{\sqrt{p}}{2} \left[\frac{ay}{p} e(\theta_y) + \frac{cy}{p} \overline{e(\theta_y)}\right] - \cos 2\pi \theta_y$

$= \pm \frac{y}{p} \frac{\sqrt{p}}{2} \left[ e(\theta_y) - \overline{e(\theta_y)}\right] - \cos 2\pi \theta_y$

$= \pm i \left[\frac{y}{p}\right] \sqrt{p} \sin 2\pi \theta_y - \cos 2\pi \theta_y,$

where (5) follows from Lemma 5.1. 

**Example 5.3.** Let $n = d = 1088 = 4^3 \cdot 17$ and consider the orbit $X$ of $r = 1$ under the action of $A = \langle 63 \rangle = \langle n - 1 \rangle$ on $\mathbb{Z}/n\mathbb{Z}$. In this situation, illustrated by Figure 8(A), holds with $J_+ = \{0, 4\} = 2Q_5 + 2$ and $J_- = \{2, 4\} = Q_3 + 3$. 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 2.1, 3.1 and 5.1 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
Figure 8. Graphs of cyclic supercharacters $\sigma_X$ of $\mathbb{Z}/n\mathbb{Z}$, where $X = A1$. Propositions 2.1, 3.1 and 5.2 can be used to produce supercharacters whose images feature elliptical patterns.

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 $\{(x_1, x_2, \ldots, x_d) : (x_1, x_2, \ldots, x_m) \in S_n\}$ 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 [15].

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

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

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

In the following, we suppose that $p$ is an odd prime number and that $|X| = d$ is a divisor of $p - 1$. Let $\omega_p$ denote a primitive $d$th root of unity modulo $p$ and let

$$S_p = \left\{ \frac{\ell}{p}(1, \omega_p, \omega_p^2, \ldots, \omega_p^{\varphi(d)-1}) : 0 \leq \ell \leq p - 1 \right\} \subseteq [0,1)^{\varphi(d)}$$
Lemma 6.2. The sets $S_p$ for $p \equiv 1 \pmod{d}$ 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

$$f(t) = a_0 + a_1t + \cdots + a_{\varphi(d)-1}t^{\varphi(d)-1}.$$

Observe that

$$\sum_{u \in S_p} e(u \cdot v) = \sum_{t=0}^{p-1} e\left(\frac{f(\omega_p)t}{p}\right) = \begin{cases} 0 & \text{if } p \nmid f(\omega_p), \\ p & \text{if } f(\omega_p). \end{cases}$$

Having fixed $d$ and $v$, we claim that the sum above is nonzero for only finitely many primes $p \equiv 1 \pmod{d}$. 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 $\mathbb{Z}/p\mathbb{Z}$ and letting $t = \omega_p$, we find that $b(\omega_p)f(\omega_p) \equiv n \pmod{p}$. This means that $p|f(\omega_p)$ implies that $p|n$, which can occur for only finitely many primes $p$. Putting this all together, we find that

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

holds for all $v$ in $\mathbb{Z}^m$. By Weyl's Criterion, it follows that the sets $S_p$ are uniformly distributed mod 1 as $p \equiv 1 \pmod{d}$ tends to infinity. \hfill $\square$

**Theorem 6.3.** If $\sigma_X$ is a cyclic supercharacter of $\mathbb{Z}/p\mathbb{Z}$, where $p$ is prime and $|X| = d$, then the image of $\sigma_X$ is contained in the image of the function $g : [0,1)^{\varphi(d)} \to \mathbb{C}$ defined by

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

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

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

(6)

(7)

For $d$ fixed, as $p$ becomes large, the image of $\sigma_X$ fills out the image of $g$ in the sense that given $\epsilon > 0$, there exists some $p \equiv 1 \pmod{d}$ such that if $\sigma_X : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ 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 $p \equiv 1 \pmod{d}$, let $A = \{1, \omega_p, \omega_p^2, \ldots, \omega_p^{d-1}\}$ be the cyclic subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ generated by a primitive $d$th root of unity $\omega_p$, and let $X = Ar$ where $p \nmid r$ so that $|X| = |A| = d$. Recall that $\{1, e(\frac{1}{d}), \ldots, e(\frac{\varphi(d)-1}{d})\}$ is a $\mathbb{Z}$-basis for the ring $\mathbb{Z}[e(\frac{1}{d}), \ldots, e(\frac{\varphi(d)-1}{d})]$. Therefore, the set $X$ is a $\mathbb{Z}$-module generated by $1, \omega, \omega^2, \ldots, \omega^{d-1}$. Consider the supercharacter $\sigma_X : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ defined by

$$\sigma_X(z) = \sum_{x \in X} e(xz).$$

(8)

(9)

(10)
of integers of the cyclotomic field \( \mathbb{Q}(\zeta_{\frac{q}{d}}) \) \[13\text{ Prop. 10.2]. For } k = 0, 1, \ldots, d - 1, \text{ the integers } b_{k,j} \text{ 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 (7). In particular, it follows that
\[
\omega_k^p \equiv \sum_{j=0}^{\varphi(d)-1} b_{k,j} \omega_p^j \pmod{p}.
\]

Letting \( y \equiv r^{-1} \ell \pmod{p} \), we have
\[
\sigma_X(y) = \sum_{x \in X} e\left(\frac{xy}{p}\right) = \sum_{k=0}^{d-1} e\left(\frac{\omega_k^p \ell}{p}\right) = \sum_{k=0}^{d-1} e\left(\sum_{j=0}^{\varphi(d)-1} b_{k,j} \omega_p^j \ell \pmod{p}\right),
\]
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 immediately from Lemma 6.2. \( \square \)

Several remarks are in order. If \( d \) is even, then \( X \) is closed under negation, so \( \sigma_X \) is real. If \( d = q^a \) where \( q \) is an odd prime, then \( g : \mathbb{T}^{\varphi(q^a)} \to \mathbb{C} \) is given by
\[
g(z_1, z_2, \ldots, z_{\varphi(d)}) = \sum_{j=1}^{\varphi(d)} z_j + \sum_{j=1}^{q-2} \prod_{j=1}^{q-2} z_{j+\ell q^{n-1}}.
\]
A particularly concrete manifestation of the preceding 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 \( \theta \mapsto (\kappa - \lambda)e^{i\theta} + \lambda e^{i(1-\kappa/\lambda)\theta} \) of the hypocycloid centered at the origin, containing the point \( \kappa \), and having precisely \( \kappa \) cusps.

**Pf. of Thm. 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 (6) 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 \[10\text{ §3]}. \( \square \)
Figure 9. Cyclic supercharacters $\sigma_X$ of $\mathbb{Z}/p\mathbb{Z}$, where $X = A_1$, whose graphs fill out $|X|$-hypocycloids.

References


Department of Mathematics, UCLA, Los Angeles, California, 90095-1555, USA
E-mail address: wduke@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