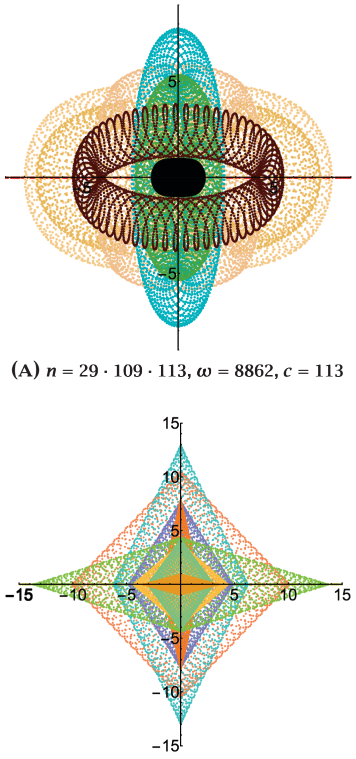
Gauss's Hidden Menagerie:
From Cyclotomy to Supercharacters

Stephan Ramon Garcia, Trevor Hyde, and Bob Lutz

At the age of eighteen, Gauss established the constructibility of the 17-gon, a result that had eluded mathematicians for two millennia. At the heart of his argument was a keen study of certain sums of complex exponentials, known now as *Gaussian periods*. These sums play starring roles in applications both classical and modern, including Kummer's development of arithmetic in the cyclotomic integers [28] and the optimized AKS primality test of H. W. Lenstra and C. Pomerance [1, 32]. In a poetic twist, this recent application of Gaussian periods realizes "Gauss's dream" of an efficient algorithm for distinguishing prime numbers from composites [24].

We seek here to study Gaussian periods from a graphical perspective. It turns out that these classical objects, when viewed appropriately, exhibit a dazzling and eclectic host of visual qualities. Some images contain discretized versions of familiar shapes, while others resemble natural phenomena. Many can be colorized to isolate certain features; for details, see "Cyclic Supercharacters."



(A) $n = 29 \cdot 109 \cdot 113$, $\omega = 8862$, $c = 113$

(B) $n = 37 \cdot 97 \cdot 113$, $\omega = 5507$, $c = 113$

Figure 1. Eye and jewel—images of *cyclic supercharacters* correspond to sets of Gaussian periods. For notation and terminology, see "Cyclic Supercharacters."

Historical Context

The problem of constructing a regular polygon with compass and straight-edge dates back to ancient times. Descartes and others knew that with only these tools on hand, the motivated geometer could draw, in principle, any segment whose length could be written as a finite composition of sums, products, and square roots of rational numbers [18]. Gauss's construction of the 17-gon relied on showing that

$$16\cos\left(\frac{2\pi}{17}\right) = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

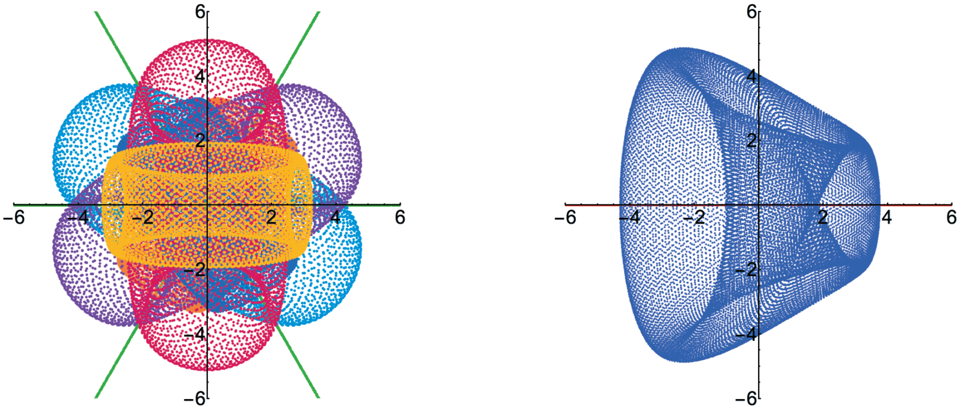
Stephan Ramon Garcia is associate professor of mathematics at Pomona College. His email address is Stephan.Garcia@pomona.edu.

Trevor Hyde is a graduate student at the University of Michigan. His email address is tghyde@umich.edu.

Bob Lutz is a graduate student at the University of Michigan. His email address is boblutz@umich.edu. *All article figures are courtesy of Bob Lutz.*

Partially supported by National Science Foundation Grant DMS-1265973.

DOI: http://dx.doi.org/10.1090/noti1269



(A) $n = 3 \cdot 5 \cdot 17 \cdot 29 \cdot 37]$, $\omega = 184747$, $c = 3 \cdot 17$

(B) $n = 13 \cdot 127 \cdot 199$, $\omega = 6077$, $c = 13$

Figure 2. Disco ball and loudspeaker—images of *cyclic supercharacters* correspond to sets of Gaussian periods. For notation and terminology, see "Cyclic Supercharacters."

was such a length. After reducing the constructibility of the n-gon to drawing the length $\cos\left(\frac{2\pi}{n}\right)$, his result followed easily. So proud was Gauss of this discovery that he wrote about it throughout his career, purportedly requesting a 17-gon in place of his epitaph.[1] While this appeal went unfulfilled, sculptor Fritz Schaper did include a 17-pointed star at the base of a monument to Gauss in Brunswick, where the latter was born [31].

Gauss went on to demonstrate that a regular n-gon is constructible if Euler's totient $\varphi(n)$ is a power of 2. He stopped short of proving that these are the only cases of constructibility; this remained unsettled until J. Petersen completed a largely neglected argument of P. Wantzel nearly three quarters of a century later [33]. Nonetheless, the chapter containing Gauss's proof has persisted deservedly as perhaps the most well-known section of his *Disquisitiones Arithmeticae*. Without the language of abstract algebra, Gauss initiated the study of *cyclotomy*, literally "circle cutting," from an algebraic point of view.

The main ingredient in Gauss's argument is an exponential sum known as a *Gaussian period*. Denoting the cardinality of a set S by $|S|$, if p is an odd prime number and ω has order d in the unit group $(\mathbb{Z}/p\mathbb{Z})^\times$, then the d-*nomial* Gaussian periods modulo p are the complex numbers

$$\sum_{j=0}^{d-1} e\left(\frac{\omega^j y}{p}\right),$$

where y belongs to $\mathbb{Z}/p\mathbb{Z}$ and $e(\theta)$ denotes $\exp(2\pi i\theta)$ for real θ. Following its appearance in *Disquisitiones*, Gauss's cyclotomy drew the attention of other mathematicians who saw its potential use in their own work. In 1879, J. J. Sylvester wrote that "[c]yclotomy is to be regarded … as the natural and inherent centre and core of the arithmetic of the future" [39]. Two of Kummer's most significant achievements depended critically on his study of Gaussian periods: Gauss's work laid the foundation for the proof of Fermat's Last Theorem in the case of regular primes and later for Kummer's celebrated reciprocity law.

This success inspired Kummer to generalize Gaussian periods in [30] to the case of composite moduli. Essential to his work was a study of the polynomial $x^d - 1$ by his former student, L. Kronecker, whom Kummer continued to mentor for the better part of both men's careers [27]. Just as Gaussian periods for prime moduli had given rise to various families of difference sets [7], Kummer's composite cyclotomy has been used to explain certain difference sets arising in finite projective geometry [14]. Shortly after Kummer's publication, L. Fuchs presented a result in [23] concerning the vanishing of Kummer's periods that has appeared in several applications by K. Mahler [34], [35]. A modern treatment of Fuchs's result and a further generalization of Gaussian periods can be found in [21].

For a positive integer n and positive divisor d of $\varphi(n)$, Kummer "defined" a d-nomial period modulo n to be the sum

$$\sum_{j=0}^{d-1} e\left(\frac{\omega^j y}{n}\right), \tag{1}$$

where ω has order d in the unit group $(\mathbb{Z}/n\mathbb{Z})^\times$ and y ranges over $\mathbb{Z}/n\mathbb{Z}$. Unlike the case of prime moduli, however, there is no guarantee that a generator ω of order d will exist or that a subgroup of order d will be unique. For example, consider $(\mathbb{Z}/8\mathbb{Z})^\times$, which contains no element of order 4, as well as three distinct subgroups of order 2. A similar lack of specificity pervaded some of Kummer's other

[1] *H. Weber makes a footnote of this anecdote in* [43, p. 362], *but omits it curiously from later editions.*

definitions, including his introduction of ideal prime factors, used to prove a weak form of prime factorization for cyclotomic integers. According to H. M. Edwards, instead of revealing deficiencies in Kummer's work, these examples suggest "the mathematical culture…as Kummer saw it" [19].

Fortunately, the ambiguity in Kummer's definition is easily resolved. For n as above and an element ω of $(\mathbb{Z}/n\mathbb{Z})^\times$, we define the Gaussian periods generated by ω modulo n to be the sums in (1), where d is the order of ω and y ranges over $\mathbb{Z}/n\mathbb{Z}$, as before. These periods are closely related to Gauss sums, another type of exponential sum [9].

Cyclic Supercharacters

In 2008, P. Diaconis and I. M. Isaacs introduced the theory of supercharacters axiomatically [15], building upon seminal work of C. André on the representation theory of unipotent matrix groups [3], [4]. Supercharacter techniques have been used to study the Hopf algebra of symmetric functions of noncommuting variables [2], random walks on upper triangular matrices [5], combinatorial properties of Schur rings [16], [40], [41], and Ramanujan sums [22].

To make an important definition, we divert briefly to the character theory of finite groups. Let G be a finite group with identity 0, $\mathcal{K}$ a partition of G, and $\mathcal{X}$ a partition of the set 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 $\sigma_X : G \to \mathbb{C}$ are called *supercharacters*, and the elements of $\mathcal{K}$ are called *superclasses*.

Since $\mathbb{Z}/n\mathbb{Z}$ is abelian, its irreducible characters are group homomorphisms $\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^\times$. Namely, for each x in $\mathbb{Z}/n\mathbb{Z}$, there is an irreducible character χ_x of $\mathbb{Z}/n\mathbb{Z}$ given by $\chi_x(y) = e(\frac{xy}{n})$. For a subgroup Γ 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 Γ. The action $a \cdot \chi_x = \chi_{a^{-1}x}$ of Γ on the irreducible characters of $\mathbb{Z}/n\mathbb{Z}$ yields a compatible partition $\mathcal{X}$ making $(\mathcal{X}, \mathcal{K})$ a supercharacter theory on $\mathbb{Z}/n\mathbb{Z}$. The corresponding supercharacters are

$$\sigma_X(y) = \sum_{x \in X} e\left(\frac{xy}{n}\right). \tag{2}$$

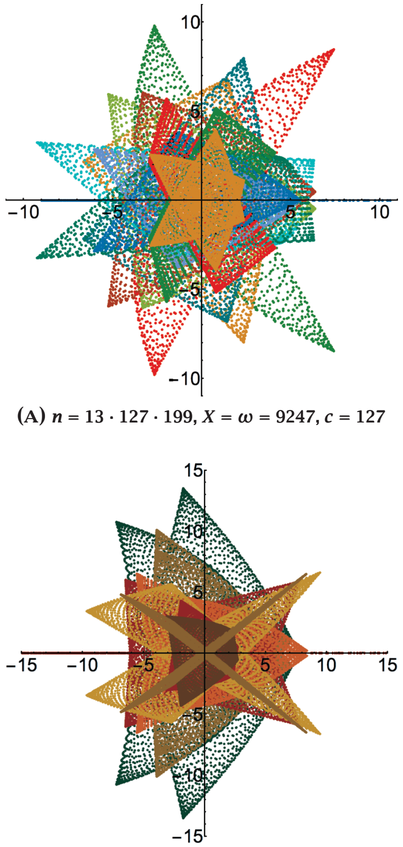
For a positive integer n and an orbit X of $\mathbb{Z}/n\mathbb{Z}$ under the multiplication action of a cyclic subgroup $\langle\omega\rangle$ of $(\mathbb{Z}/n\mathbb{Z})^\times$, we define the *cyclic supercharacter* $\sigma_X : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ by (2). The values of these functions are Gaussian periods in the sense of Kummer [17]. For applications of supercharacter theory to other exponential sums, see [11], [12], [22].

We are now in a position to clarify the captions and colorizations of the numerous figures. Unless specified otherwise, the image appearing in each figure is the image in $\mathbb{C}$ of the cyclic supercharacter $\sigma_{\langle\omega\rangle} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$, where ω belongs to $(\mathbb{Z}/n\mathbb{Z})^\times$, and $\langle\omega\rangle = \langle\omega\rangle 1$ denotes the orbit of 1 under the action of the subgroup generated by ω. Conveniently, the image of *any* cyclic supercharacter is a scaled subset of the image of one having the form $\sigma_{\langle\omega\rangle}$ [17, Proposition 2.2], so a restriction of our attention to orbits of 1 is natural. Moreover, the image of $\sigma_{\langle\omega\rangle}$ is the set of Gaussian periods generated by ω modulo n, bringing classical relevance to these figures.

To colorize each image, we fix a proper divisor c of n and assign a color to each of the *layers*,

$$\{\sigma_{\langle\omega\rangle 1}(y) \mid y \equiv j \pmod{c}\},$$

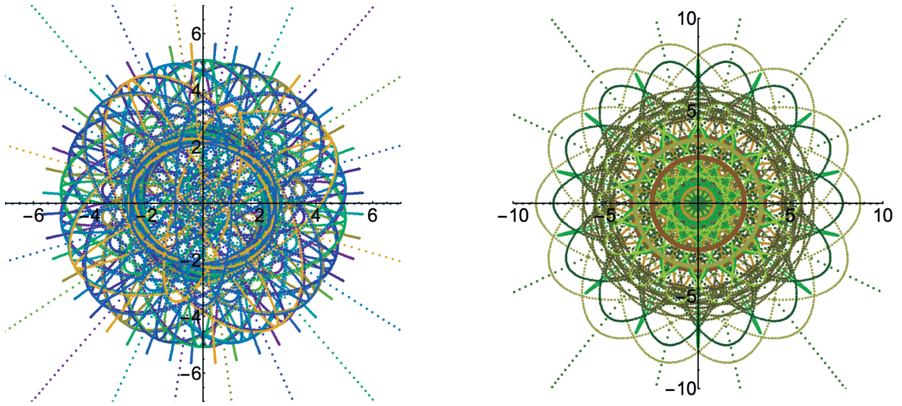
for $j = 0, 1, \ldots, c-1$. Different choices of c result in different "layerings." For many images, certain values of c yield colorizations that separate distinct graphical components.



(A) $n = 13 \cdot 127 \cdot 199$, $X = \omega = 9247$, $c = 127$

(B) $n = 3 \cdot 7 \cdot 211 \cdot 223$, $\omega = 710216$, $c = 211$

Figure 3. Mite and moth—images of *cyclic supercharacters* correspond to sets of Gaussian periods. For notation and terminology, see "Cyclic Supercharacters."



(A) $n = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$, $\omega = 254$, $c = 11$

(B) $n = 3^2 \cdot 5^2 \cdot 7 \cdot 17^2$, $\omega = 3599$, $c = 17^2$

Figure 4. Atoms—images of *cyclic supercharacters* correspond to sets of Gaussian periods. For notation and terminology, see "Cyclic Supercharacters."

Predictable layering occurs when the image of a cyclic supercharacter contains several rotated copies of a proper subset. We say that a subset of $\mathbb{C}$ has *k-fold dihedral symmetry* if it is invariant under complex conjugation and rotation by $\frac{2\pi}{k}$ about the origin. For example, the image pictured in Figure 4(A) has 11-fold dihedral symmetry, while the symmetry in Figure 4(B) is 7-fold. The image of a cyclic supercharacter $\sigma_{\langle\omega\rangle} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ has k-fold dihedral symmetry, where $k = \gcd(n, \omega - 1)$ [17, Proposition 3.1]. In this situation, taking $c = k$ results in exactly k layers that are rotated copies of one another.

In addition to the behaviors above, certain cyclic supercharacters enjoy a multiplicative property [17, Theorem 2.1]. Specifically, if $\gcd(m, n) = 1$ and $\omega \mapsto (\omega_m, \omega_n)$ under the isomorphism $(\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ afforded by the Chinese Remainder Theorem, where the multiplicative orders of ω_m and ω_n are coprime, then

$$(3)\quad \sigma_{\langle\omega\rangle}(\mathbb{Z}/mn\mathbb{Z}) = \{wz \in \mathbb{C} : (w, z) \in \sigma_{\langle\omega_m\rangle}(\mathbb{Z}/m\mathbb{Z}) \times \sigma_{\langle\omega_n\rangle}(\mathbb{Z}/n\mathbb{Z})\}.$$

This can be used to explain the images of cyclic supercharacters featuring "nested" copies of a given shape. For examples of this phenomenon, see Figures 6 and 7.

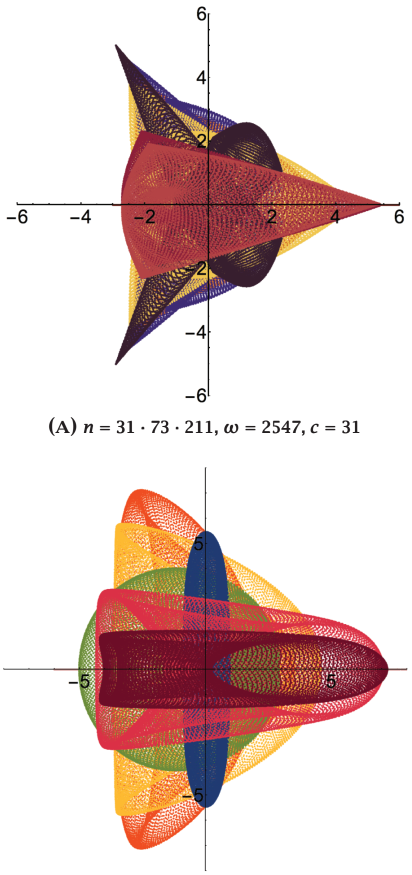
Asymptotic Behavior

In this section, we restrict our attention to cyclic supercharacters $\sigma_X : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, where q is a power of an odd prime and $X = \langle\omega\rangle$ is an orbit of 1. The Gaussian periods attained as values of these supercharacters have been applied in various settings [6], [8], [26]. Plotting the functions σ_X in this case reveals asymptotic patterns that have, until recently, gone unseen. Before proceeding, we recall several definitions and results.

Uniform Distribution mod 1

Let m be a positive integer and Λ a finite subset of $\mathbb{R}^m$. We write

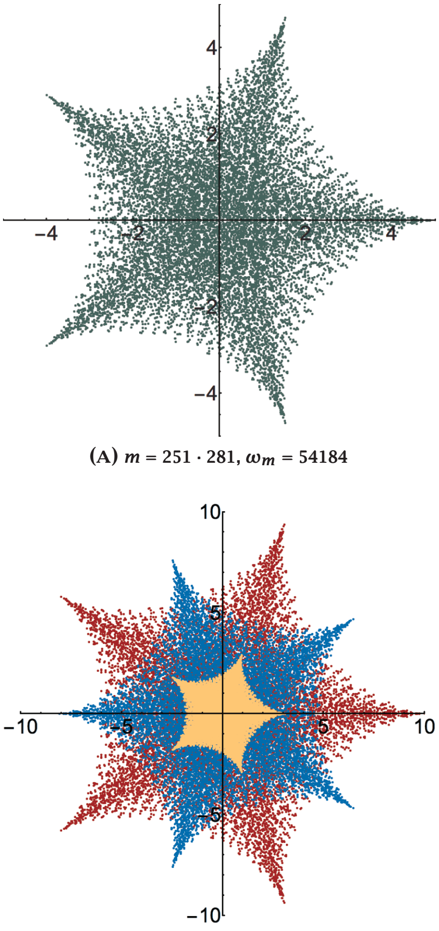
$$\widehat{\Lambda} = \{(\lambda_1 - \lfloor\lambda_1\rfloor, \ldots, \lambda_m - \lfloor\lambda_m\rfloor) \in [0,1)^m : (\lambda_1, \ldots, \lambda_m) \in \Lambda\},$$



(A) $n = 31 \cdot 73 \cdot 211$, $\omega = 2547$, $c = 31$

(B) $n = 3 \cdot 31 \cdot 73 \cdot 211$, $\omega = 1463$, $c = 73$

Figure 5. Bird and spacecraft—images of cyclic supercharacters.



(A) $m = 251 \cdot 281$, $\omega_m = 54184$

(B) $m = 251 \cdot 281$, $\omega_m = 54184$

Figure 6. The image on the top is the product set of the image on the bottom and the image $\{2, \frac{1}{2}(\pm\sqrt{5} - 1)\}$, as in (3).

where $\lfloor \cdot \rfloor$ denotes the greatest integer function. The *discrepancy* of the set Λ is

$$\sup_B \left| \frac{|B \cap \widehat{\Lambda}|}{|\widehat{\Lambda}|} - \operatorname{vol}(B) \right|,$$

where the supremum is taken over all boxes $B = [a_1, b_1) \times \cdots \times [a_m, b_m) \subset [0,1)^m$ and $\operatorname{vol}(B)$ denotes the volume of B. We say that a sequence $(\Lambda_n)_{n=1}^{\infty}$ of finite subsets of $\mathbb{R}^m$ is *uniformly distributed mod* 1 if the discrepancy of Λ_n tends to zero as $n \to \infty$.

Many accessible examples exist in the case $m = 1$. For instance, a well-known theorem of Weyl states that if α is an irrational number, then the sequence

$$(4) \qquad (\{k\alpha \in \mathbb{R} : k = 0, 1, \ldots, n-1\})_{n=1}^{\infty}$$

is uniformly distributed mod 1 [44]. A lovely result of Vinogradov is that the same holds when k above is replaced by the kth prime number [42]. While it is known that the sequence

$$(\{\theta, \theta^2, \ldots, \theta^n\})_{n=1}^{\infty}$$

is uniformly distributed mod 1 for almost every $\theta > 1$, specific cases such as $\theta = \frac{3}{2}$ are not well understood [20]. Surprisingly perhaps, the sequence

$$(\{\log 1, \log 2, \ldots, \log n\})_{n=1}^{\infty}$$

is not uniformly distributed mod 1. This example and several others are elaborated in [29] using the following crucial characterization, also due to Weyl [45].

Lemma 1 (Weyl's criterion). *A sequence $(\Lambda_n)_{n=1}^{\infty}$ of finite subsets of $\mathbb{R}^m$ is uniformly distributed mod* 1 *if and only if for each $\mathbf{v}$ in $\mathbb{Z}^m$ we have*

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

For example, let $(\Lambda_n)_{n=1}^{\infty}$ be the sequence in (4). Since α is irrational,

$$\frac{1}{|\Lambda_n|} \sum_{u\in\Lambda_n} e(uv) = \frac{1}{n}\sum_{k=0}^{n-1} e(v\alpha)^k = \frac{1}{n}\left(\frac{1-e(v\alpha)^n}{1-e(v\alpha)}\right)$$

for each nonzero $v \in \mathbb{Z}$. Consequently,

$$\left| \frac{1}{n}\left(\frac{1-e(v\alpha)^n}{1-e(v\alpha)}\right) \right| \leq \frac{1}{n}\frac{2}{|1-e(v\alpha)|} \to 0$$

as $n \to \infty$, so Lemma 1 confirms that (4) is uniformly distributed mod 1.

Cyclotomic Polynomials

For a positive integer d, the *dth cyclotomic polynomial* $\Phi_d(x)$ is defined by the formula

$$\Phi_d(x) = \prod_{\substack{k=1,2,\ldots,d \\ \gcd(k,d)=1}} \left(x - e\left(\tfrac{k}{d}\right)\right).$$

It can be shown that $\Phi_d(x)$ is of degree $\varphi(d)$ and belongs to $\mathbb{Z}[x]$. In *Disquisitiones*, Gauss showed that $\Phi_d(x)$ is irreducible, hence the minimal polynomial of any primitive dth root of unity, over $\mathbb{Q}$. The first several cyclotomic polynomials are

$$\begin{aligned}
\Phi_1(t) &= x - 1, \\
\Phi_2(t) &= x + 1, \\
\Phi_3(t) &= x^2 + x + 1, \\
\Phi_4(t) &= x^2 + 1, \\
\Phi_5(t) &= x^4 + x^3 + x^2 + x + 1.
\end{aligned}$$

In these examples, the coefficients have absolute value at most 1. In 1938, N. G. Chebotarëv asked

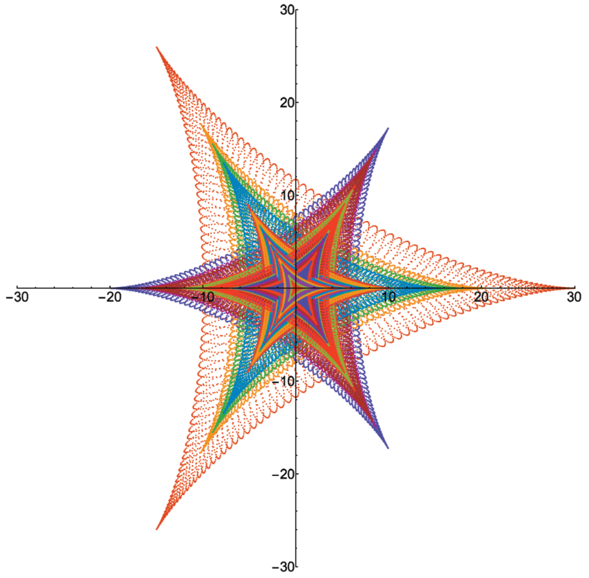


Figure 7. $n = 127^2 \cdot 401$, $\omega = 6085605$, $c = 401$

whether this phenomenon continues for all factors of $x^d - 1$ and all values of d [25]. Three years later, V. Ivanov showed that while the pattern holds for $d < 105$, one coefficient of $\Phi_{105}(x)$ is -2. Unbeknownst to either mathematician, A. S. Bang had solved Chebotarëv's challenge more than forty years earlier [10].

Main Theorem

We require a lemma essentially due to G. Myerson. The original aim of the result was to count the number of ways to write an arbitrary element of $(\mathbb{Z}/q\mathbb{Z})^\times$ as a sum of elements, one in each coset of a fixed subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$. For our purposes, Myerson's lemma will be critical in discussing the asymptotic behavior of the images of cyclic supercharacters. Throughout, we let ω_q denote a primitive dth root of unity in $\mathbb{Z}/q\mathbb{Z}$, in which $q = p^a$ is a power of an odd prime p, and

$$\Lambda_q = \left\{ \frac{\ell}{q}\left(1, \omega_q, \omega_q^2, \ldots, \omega_q^{\varphi(d)-1}\right) \in [0,1)^{\varphi(d)} \right. \\ \left. : \ell = 0, 1, \ldots, q-1 \right\}. \tag{5}$$

Lemma 2 (Myerson [36]). *The sequence $(\Lambda_q)_{q \equiv 1 \pmod d}$ is uniformly distributed mod 1.*

Proof. Let $\mathbf{v} = (v_0, \ldots, v_{\varphi(d)-1})$ be nonzero in $\mathbb{Z}^{\varphi(d)}$ and let $f \in \mathbb{Z}[x]$ be given by

$$f(x) = v_0 + v_1 x + \cdots + v_{\varphi(d)-1} x^{\varphi(d)-1}.$$

Writing $r = \frac{q}{\gcd(q, f(\omega_q))}$, we notice that

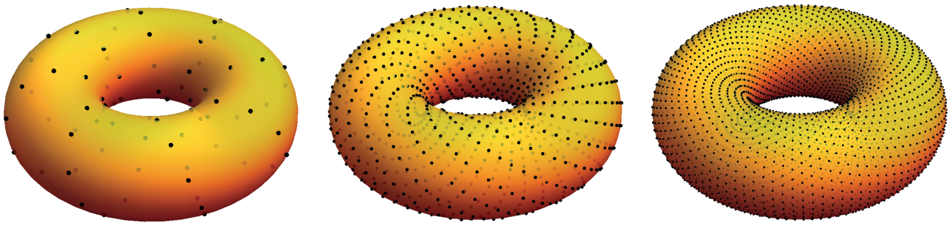
$$\begin{aligned} \sum_{\mathbf{u} \in \Lambda_q} e(\mathbf{u} \cdot \mathbf{v}) &= \sum_{\ell=0}^{q-1} e\left(\frac{\ell f(\omega_q)}{q}\right) \\ &= \sum_{k=0}^{q/r-1} \sum_{j=0}^{r-1} e\left(\frac{(kr+j) f(\omega_q)}{q}\right) \\ &= \sum_{k=0}^{q/r-1} \sum_{j=0}^{r-1} e\left(\frac{k f(\omega_q)}{\gcd(q, f(\omega_q))} + \frac{j f(\omega_q)}{q}\right) \\ &= \sum_{k=0}^{q/r-1} \sum_{j=0}^{r-1} e\left(\frac{j f(\omega_q)}{q}\right) \\ &= \frac{q}{r} \sum_{j=0}^{r-1} e\left(\frac{j f(\omega_q)}{q}\right) \\ &= \begin{cases} q & \text{if } q | f(\omega_q), \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{6}$$

Since $\Phi_d(x)$ is irreducible over $\mathbb{Q}$ and of greater degree than $f(x)$, we see that $\gcd(f(x), \Phi_d(x)) = 1$ in $\mathbb{Q}[x]$. From this we obtain $a(x)$ and $b(x)$ in $\mathbb{Z}[x]$ such that $a(x)f(x) + b(x)\Phi_d(x) = s$ for some $s \in \mathbb{Z}$. Evaluating at $x = \omega_q$ reveals that $a(\omega_q)f(\omega_q) \equiv s \pmod q$, so $q|s$ whenever $q|f(\omega_q)$. Hence $q|f(\omega_q)$ for at most finitely many odd prime powers $q \equiv 1 \pmod d$. It follows from (6) that

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

Appealing to Lemma 1 completes the proof. □

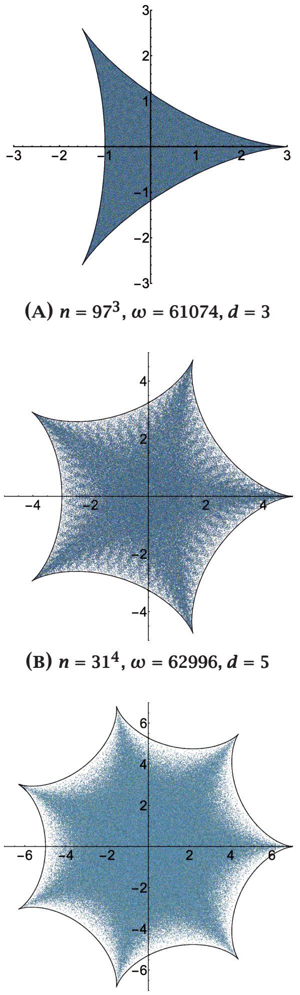
The following theorem summarizes our current understanding of the asymptotic behavior of cyclic supercharacters. A special case supplies a



(A) $q = 73$ (B) $q = 31^2$ (C) $q = 3571$

Figure 8. The sequence $(\Lambda_q)_{q \equiv 1 \,(\mathrm{mod}\ 3)}$, defined in (5), is uniformly distributed mod 1. Here we plot several of the sets $\Lambda_q \subset [0,1)^2$, identifying $[0,1)^2$ with a torus.

geometric description of the set of $|X|$-nomial periods modulo p considered by Gauss, shedding new light on these classical objects. We let $\mathbb{T}$ denote the unit circle in $\mathbb{C}$.



(A) $n = 97^3, \omega = 61074, d = 3$

(B) $n = 31^4, \omega = 62996, d = 5$

(C) $n = 1933^2, \omega = 537832, d = 7$

Figure 9. Certain cyclic supercharacters fill out regions bounded by *hypocycloids*, outlined in black (see Proposition 1).

Theorem 1 (Duke-Garcia-Lutz). *If $\sigma_X : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ is a cyclic supercharacter, where $q = p^a$ is a power of an odd prime, X is an orbit of 1, and $|X| = d$ divides $p-1$, then the image of σ_X is contained in the image of the Laurent polynomial function $g_d : \mathbb{T}^{\varphi(d)} \to \mathbb{C}$ defined by*

$$g_d(z_1, z_2, \ldots, z_{\varphi(d)}) = \sum_{k=0}^{d-1} \prod_{j=0}^{\varphi(d)-1} z_{j+1}^{c_{jk}}, \tag{7}$$

where the c_{jk} are given by the relation

$$x^k \equiv \sum_{j=0}^{\varphi(d)-1} c_{jk} x^j \pmod{\Phi_d(x)}. \tag{8}$$

Moreover, for a fixed $|X| = d$, as $q \equiv 1 \pmod d$ tends to infinity, every nonempty open disk in the image of g eventually contains points in the image $\sigma_X(\mathbb{Z}/q\mathbb{Z})$.

Proof. Since the elements $1, \omega_q, \ldots, \omega_q^{\varphi(d)-1}$ form a $\mathbb{Z}$-basis for $\mathbb{Z}[\omega_q]$ [37, p. 60], for $k = 0, 1, \ldots, d-1$ we can write

$$\omega_q^k \equiv \sum_{j=0}^{\varphi(d)-1} c_{jk} \omega_p^j \pmod q,$$

where the integers c_{jk} are given by (8). Letting $X = \langle \omega_q \rangle$, we see that

$$\begin{aligned}\sigma_X(y) &= \sum_{x \in X} e\left(\frac{xy}{q}\right) = \sum_{k=0}^{d-1} e\left(\frac{\omega_q^k y}{q}\right)\\ &= \sum_{k=0}^{d-1} e\left(\sum_{j=0}^{\varphi(d)-1} c_{jk} \frac{\omega_q^j y}{q}\right)\\ &= \sum_{k=0}^{d-1} \prod_{j=0}^{\varphi(d)-1} e\left(\frac{\omega_q^j y}{q}\right)^{c_{jk}},\end{aligned}$$

whence the image of σ_X is contained in the image of the function $g_d : \mathbb{T}^{\varphi(d)} \to \mathbb{C}$ defined in (7). The claim about open disks follows immediately from Lemma 2. □

Several remarks are in order. First, when the hypotheses of Theorem 1 are satisfied, we say that σ_X *fills out* the image of g_d, as illustrated by Figure 9. The corresponding values of d are given in captions. Second, since every divisor of $\varphi(q) = p^{a-1}(p-1)$ is the cardinality of some orbit X under the action of a cyclic subgroup of $(\mathbb{Z}/p^a\mathbb{Z})^\times$, the requirement that $|X|$ divide $p-1$ might seem restrictive. However, it turns out that if p divides $|X|$, then the image of σ_X is equal to a scaled copy of the image of a supercharacter that satisfies the hypotheses of the theorem, except for a single point at the origin [17, Proposition 2.4].

Examples

As a consequence of Theorem 1, the functions g_d are instrumental in understanding the asymptotic behavior of cyclic supercharacters $\sigma_X : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, where q is a power of an odd prime. Fortunately, whenever the coefficients of $\Phi_d(x)$ are relatively accessible, we can obtain a convenient formula for g_d. For example, it is not difficult to show that

$$\Phi_{2^b}(x) = x^{2^{b-1}} + 1,$$

for any positive integer b. With this, we can compute the integers c_{jk} in (8) to see that

$$g_{2^b}(z_1, z_2, \ldots, z_{2^{b-1}}) = 2\sum_{j=1}^{2^{b-1}} \Re(z_j),$$

where $\Re(z)$ denotes the real part of z. Hence the image of g_{2^b} is the real interval $[-2^b, 2^b]$. Alternatively, if r is an odd prime, then

$$\Phi_{2r}(x) = \sum_{j=0}^{r-1} (-x)^j,$$

giving

$$g_{2r}(z_1, z_2, \ldots, z_{r-1}) = 2\Re\left(\frac{z_2 z_4 \cdots z_{r-1}}{z_1 z_3 \cdots z_{r-2}}\right) + 2\sum_{j=1}^{r-1} \Re(z_j).$$

More generally, g_d is real valued whenever d is even.

A novel and particularly accessible behavior occurs when $d = r$ is an odd prime. The reader might recall that a *hypocycloid* is a planar curve obtained by tracing a fixed point on a circle of integral radius as it "rolls" within a larger circle of integral radius. Figure 10 illustrates this construction. We are interested in the hypocycloid that is centered at the origin and has r cusps, one of which is at r. This curve is obtained by rolling a circle of radius 1 within a circle of radius d; it has the parametrization $\theta \mapsto (r-1)e(\theta) + e((1-r)\theta)$. Let H_r denote the compact region bounded by this curve.

Proposition 1. *If r is an odd prime, then the image of g_r is H_r.*

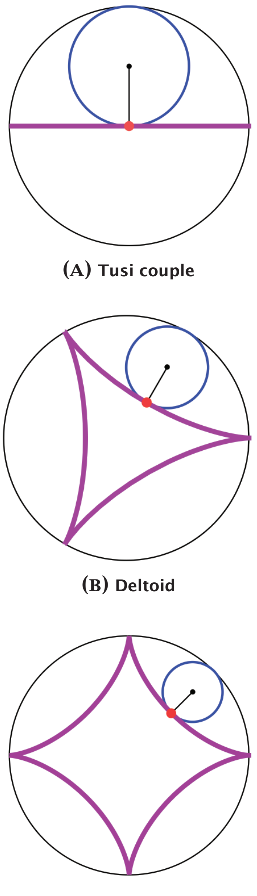
Proof. Since

$$\Phi_r(x) = x^{r-1} + x^{r-2} + \cdots + x + 1,$$

we obtain the formula

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

The image of this map is the set of all traces of matrices in $SU(r)$, the group of $r \times r$ complex unitary matrices with determinant 1. This set is none other than H_r [13, Theorem 3.2.3]. In particular, the image under g_d of the diagonal $z_1 = z_2 = \cdots = z_{r-1}$ is the boundary of H_r. □


(A) Tusi couple

(B) Deltoid

(C) Astroid

Figure 10. Circles of radius 1 trace out hypocycloids as they roll within circles of radii (from top to bottom) 2, 3, and 4.

To expand on the previous example, suppose again that r is an odd prime and b is a positive integer. We have

$$\Phi_{r^b}(x) = \sum_{j=0}^{r-1} x^{jr^{b-1}},$$

whence

$$g_{r^b}(z_1, z_2, \dots, z_{r^b - r^{b-1}}) = \sum_{j=1}^{r^b - r^{b-1}} z_j + \sum_{j=1}^{r^{b-1}} \prod_{\ell=0}^{r-2} z_{j+\ell r^{b-1}}^{-1}. \tag{9}$$

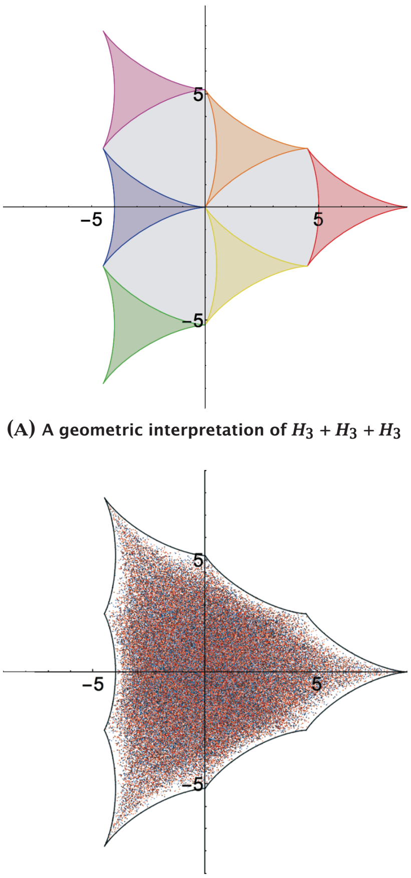
If $r = 3$ and $b = 2$, for instance, then the map is given by

$$\begin{aligned} g_9(z_1, z_2, z_3, z_4, z_5, z_6) &= z_1 + z_4 + \frac{1}{z_1 z_4} + z_2 + z_5 + \frac{1}{z_2 z_5} \\ &\quad + z_3 + z_6 + \frac{1}{z_3 z_6}. \end{aligned}$$

A definition will enable us to discuss the image in this situation. The *Minkowski sum* of two nonempty subsets S and T of $\mathbb{C}$, denoted by $S + T$, is the set

$$S + T = \{s + t \in \mathbb{C} : s \in S \text{ and } t \in T\}.$$

The Minkowski sum of an arbitrary finite collection is defined by induction. As a consequence of Proposition 1, we discover that the image of g_9 is none other than the Minkowski sum $H_3 + H_3 + H_3$, as illustrated in Figure 11. A close look at (9) reveals a more general phenomenon.



(A) A geometric interpretation of $H_3 + H_3 + H_3$

(B) $n = 1009^2$, $\omega = 84669$, $d = 3^2$

Figure 11. The supercharacter at the top fills out a Minkowski sum of filled deltoids.

Corollary 1. *If r^b is a power of an odd prime, then the image of g_{r^b} is the Minkowski sum*

$$\sum_{j=1}^{r^{b-1}} H_r.$$

The Shapley-Folkman-Starr Theorem, familiar to mathematical economists, gives an explicit upper bound on the distance between points in a Minkowski sum and its convex hull [38]. In the context of Corollary 1, we obtain the bound

$$\min\{|w - z| : w \in \sum_{j=1}^{r^{b-1}} H_r\} \le 2\sqrt{2} r \sin\left(\frac{\pi}{r}\right),$$

for any z in the filled r-gon with vertices at $r^b e(\frac{j}{r})$ for $j = 1, 2, \dots, r$. It follows easily that as $b \to \infty$, any point in the filled r-gon whose vertices are the rth roots of unity becomes arbitrarily close to points in the scaled Minkowski sum

$$\frac{1}{r^{b-1}} \sum_{j=1}^{r^{b-1}} H_r.$$

Concluding Remarks

There is work to be done toward understanding the images of cyclic supercharacters. If we are to stay the course of inquiry set in the Examples section, then a different approach is required; beyond the special cases discussed above, a general formula for the integers c_{jk} in (8) appears unobtainable, since there is no known simple closed-form expression for the coefficients of an arbitrary cyclotomic polynomial $\Phi_d(x)$.

There is, however, a remedy. To minimize headache, suppose that $d = rs$ is a product of distinct odd primes and that $\omega_q \mapsto (\gamma_r, \gamma_s)$ under the standard isomorphism $(\mathbb{Z}/d\mathbb{Z})^\times \to (\mathbb{Z}/r\mathbb{Z})^\times \times (\mathbb{Z}/s\mathbb{Z})^\times$. Instead of wielding the elements $1, \omega_q, \dots, \omega_q^{\varphi(d)-1}$ as a $\mathbb{Z}$-basis for $\mathbb{Z}[\omega_q]$, we can use an analogous basis for $\mathbb{Z}[\gamma_r, \gamma_s]$. After some computation, we see that the image of the function g_d, formerly quite mysterious, is equal to the image of the function $h_d : \mathbb{T}^{\varphi(d)} \to \mathbb{C}$ given by

$$\begin{aligned} h\big((z_{ij})_{0 \le i < r-1,\, 0 \le j < s-1}\big) &= \sum_{i=0}^{r-2} \sum_{j=1}^{s-2} z_{ij} + \sum_{i=0}^{r-2} \prod_{j=0}^{s-2} \frac{1}{z_{ij}} \\ &\quad + \sum_{j=0}^{s-2} \prod_{i=0}^{r-2} \frac{1}{z_{ij}} + \prod_{i=0}^{r-2} \prod_{j=0}^{s-2} z_{ij}. \end{aligned} \tag{10}$$

This procedure, which amounts to a change of coordinates, can be used to obtain a closed formula for a Laurent polynomial map h_d having the same image as g_d, for any integer d. This brings us one step closer to understanding the asymptotic behavior of the cyclic supercharacters in "Asymptotic Behavior." In practice, however, the functions h_d are still difficult to analyze, despite being considerably easier to write down than the g_d. Even the simplest cases, described in (10), resist the accessible geometric description provided in the preceding section.

While certain graphical features of cyclic supercharacters with composite moduli have been explained in [17], the mechanisms behind many of the striking patterns herein remain enigmatic. An important step toward deciphering the behavior of these supercharacters is to predict the layering constant c, discussed in "Cyclic Supercharacters," given only a modulus n and generator ω. As is apparent, these layerings betray an underlying geometric structure that allows us to decompose the images of σ_X into more manageable sets. We have been successful so far in finding appropriate values of c ad hoc; however, a general theory is necessary to formalize our intuition.

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in p, *Annals of Mathematics*, 160(2):781–793, 2004.

[2] Marcelo Aguiar, et. al., Supercharacters, symmetric functions in noncommuting variables, and related Hopf algebras, *Adv. Math.*, 229:2310–2337, 2012.

[3] Carlos A. M. André, The basic character table of the unitriangular group, *J. Algebra*, 241(1):437–471, 2001. dx.doi.org/10.1006/jabr.2001.8734, DOI:10.1006/jabr.2001.8734.

[4] ______, Basic characters of the unitriangular group, *J. Algebra*, 175(1):287–319, 1995. dx.doi.org/10.1006/jabr.1995.1187, DOI:10.1006/jabr.1995.1187.

[5] Ery Arias-Castro, Persi Diaconis, and Richard Stanley, A super-class walk on upper-triangular matrices, *J. Algebra*, 278(2):739–765, 2004. dx.doi.org/10.1016/j.jalgebra.2004.04.005, DOI:10.1016/j.jalgebra.2004.04.005.

[6] L. D. Baumert, W. H. Mills, and Robert L. Ward, Uniform cyclotomy, *Journal of Number Theory*, 14(1):67–82, 1982.

[7] Leonard D. Baumert, *Cyclic Difference Sets*, Springer, 1971.

[8] Eva Bayer-Fluckiger and Piotr Maciak, Upper bounds for the Euclidean minima of abelian fields of odd prime power conductor, *Mathematische Annalen*, 357(3):1071–1089, 2013.

[9] Bruce C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Wiley, 1998.

[10] D. M. Bloom, On the coefficients of the cyclotomic polynomials, *The American Mathematical Monthly*, 75(4):372–377, 1968.

[11] J. L. Brumbaugh, Madeleine Bulkow, Luis Alberto Garcia German, Stephan Ramon Garcia, Matt Michal, and Andrew P. Turner, The graphic nature of the symmetric group, *Experimental Mathematics*, 22(4):421–442, 2013.

[12] J. L. Brumbaugh, Madeleine Bulkow, Patrick S. Fleming, Luis Alberto Garcia German, Stephan Ramon Garcia, Gizem Karaali, Matt Michal, Andrew P. Turner, and Hong Suh, Supercharacters, exponential sums, and the uncertainty principle, *Journal of Number Theory*, 144(0):151–175, 2014.

[13] Barrie Cooper, *Almost Koszul duality and rational conformal field theory*, PhD thesis, University of Bath, 2007.

[14] D. H. Lehmer and Emma Lehmer, Cyclotomy for nonsquarefree moduli, Marvin I. Knopp, editor, *Analytic Number Theory*, volume 899 of Lecture Notes in Mathematics, Springer, Berlin-Heidelberg, 1981, pp. 276–300.

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

[16] Persi Diaconis and Nathaniel Thiem, Supercharacter formulas for pattern groups, *Trans. Amer. Math. Soc.*, 361(7):3501–3533, 2009. dx.doi.org/10.1090/S0002-9947-09-04521-8, DOI:10.1090/S0002-9947-09-04521-8.

[17] William Duke, Stephan Ramon Garcia, and Bob Lutz, The graphic nature of Gaussian periods, *Proc. Amer. Math. Soc.*, 143(5):1849–1863, 2015. dx.doi.org/10.1090/S0002-9939-2015-12322-2, DOI:10.1090/S0002-9939-2015-12322-2.

[18] William Dunham, 1996—a triple anniversary, *Math Horizons*, 4(1):8–13, 1996.

[19] Harold M. Edwards, Mathematical ideas, ideals, and ideology, *The Mathematical Intelligencer*, 14(2):6–19, 1992.

[20] Noam D. Elkies and Curtis T. McMullen, Gaps in $n \bmod 1$ and ergodic theory, *Duke Math. J.*, 123(1):95–139, 05 2004. dx.doi.org/10.1215/S0012-7094-04-12314-0, DOI:10.1215/S0012-7094-04-12314-0.

[21] Ronald J. Evans, Generalized cyclotomic periods, *Proc. Amer. Math. Soc.*, 81(2):207–212, 1981.

[22] Christopher F. Fowler, Stephan Ramon Garcia, and Gizem Karaali, Ramanujan sums as supercharacters, *The Ramanujan Journal*, 35(2):205–241, 2014.

[23] L. Fuchs, Ueber die perioden, welche aus den wurzeln der gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte zahl ist, *Journal reine angew. Math.*, 61:374–386, 1863.

[24] Andrew Granville, It is easy to determine whether a given integer is prime, *Bull. Amer. Math. Soc.*, 42(1):3–38, 2005.

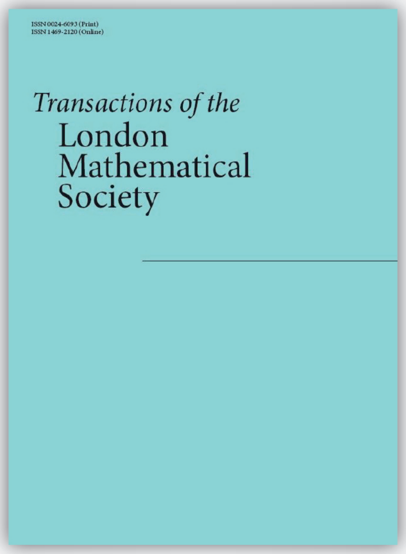
[25] Richard Grassl and Tabitha T. Y. Mingus, Cyclotomic polynomial factors, *The Mathematical Gazette*, 89(515):195–201, 2005.

[26] Akinari Hoshi, Explicit lifts of quintic Jacobi sums and period polynomials for $\mathbf{F}_q$, *Proc. Japan Acad. Ser. A Math. Sci.*, 82(7):87–92, 10 2006.

[27] I. M. James, *Driven to Innovate: A Century of Jewish Mathematicians and Physicists*, Peter Lang Series.,Peter Lang, 2009.

[28] A. N. Kolmogorov and A. A. P. Yushkevich, *Mathematics of the 19th Century: Vol. II: Geometry, Analytic Function Theory*, 1996.

[29] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Dover Books on Mathematics, Dover Publications, 2012. books.google.com/books?id=mnY8LpyXHM0C.



[30] Ernst Kummer, Theorie der idealen primfaktoren der complexen zahlen, welche aus den wurzeln der gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengestzte zahl ist, *Abhandlungen der Königlichen Akademie der Wissenschaften in Berlin*, pages 1–47, 1856.

[31] Hendrik W. Lenstra and Gerard van der Geer, The mathematical tourist, *The Mathematical Intelligencer*, 9(2):44–45, 1987.

[32] H. W. Lenstra, Primality testing with Gaussian periods, Manindra Agrawal and Anil Seth, editors, *FST TCS 2002: Foundations of Software Technology and Theoretical Computer Science*, volume 2556 of Lecture Notes in Computer Science, Springer, Berlin-Heidelberg, 2002, p. 1.

[33] Jesper Lützen, Why was Wantzel overlooked for a century? The changing importance of an impossibility result, *Historia Mathematica*, 36(4):374–394, 2009.

[34] K. Mahler, On a special function, *Journal of Number Theory*, 12(1):20–26, 1980.

[35] ———, On the zeros of a special sequence of polynomials, *Math. of Comp.*, 39(159):207–212, 1982.

[36] Gerald Myerson, A combinatorial problem in finite fields, II, *The Quarterly Journal of Mathematics*, 31(2):219–231, 1980.

[37] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, Springer-Verlag, 1999.

[38] Ross M. Starr, Quasi-equilibria in markets with nonconvex preferences, *Econometrica*, 37(1):25–38, 1969.

[39] James Joseph Sylvester, On certain ternary cubic-form equations, *The Collected Mathematical Papers of James Joseph Sylvester, Volume III*, American Mathematical Society, 2008, p. 312–391.

[40] Nathaniel Thiem, Branching rules in the ring of superclass functions of unipotent upper-triangular matrices, *J. Algebraic Combin.*, 31(2):267–298, 2010 `dx.doi.org/10.1007/s10801-009-0186-z`, DOI: `10.1007/s10801-009-0186-z`.

[41] Nathaniel Thiem and Vidya Venkateswaran, Restricting supercharacters of the finite group of unipotent uppertriangular matrices. *Electron. J. Combin.*, 16(1):Research Paper 23, 32, 2009. `www.combinatorics.org/Volume_16/Abstracts/v16i1r23.html`.

[42] I. M. Vinogradov, On an estimate of trigonometric sums with prime numbers, *Izv. Akad. Nauk SSSR Ser. Mat.*, 12(3):225–248, 1948.

[43] Heinrich Weber, *Encyklopädie der Elementaren Algebra und Analysis*, B. G. Teubner, second edition, 1906.

[44] Hermann Weyl, Über die gibbssche erscheinung und verwandte konvergenzphänomene, *Rendiconti del Circolo Matematico di Palermo*, 30(1):377–407, 1910. `dx.doi.org/10.1007/BF03014883`, DOI:`10.1007/BF03014883`.

[45] ———, Über die Gleichverteilung von Zahlen mod. Eins, *Mathematische Annalen*, 77(3):313–352, 1916.