Visual Aspects of Gaussian Periods and Analogues

by

SAMANTHA NICOLE PLATT

A dissertation accepted and approved in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
in Mathematics

Dissertation Committee:
Ellen Eischen, Chair
Nicolas Addington, Core Member
Yefeng Shen, Core Member
Benjamin Young, Core Member
Woan Foong Wong, Institutional Representative

University of Oregon
Spring 2024

DISSERTATION ABSTRACT

Samantha Nicole Platt

Doctor of Philosophy in Mathematics

Title: Visual Aspects of Gaussian Periods and Analogues

In this dissertation, we study Gaussian periods and their analogues from a visual perspective. Building on the work of Duke, Garcia, Hyde, Lutz, and others [BBF$^+$14, BBGG$^+$13, DGL15, GHL15], we introduce a more dynamical study of Gaussian periods, and we prove an explicit bound on the value of Gaussian periods using this framework. Additionally, we generalize the construction of Gaussian periods using the perspective of supercharacter theory. Using this new construction, we prove a result which greatly generalizes the main theorem of [DGL15]. We also initiate the visual study of Gaussian periods from the perspective of number theory and class field theory, and we define a generalized construction of Gaussian periods using this perspective. We discuss this class field theory analogue in depth when the base field is quadratic imaginary.

The work presented here includes and expands upon a paper by this author [Pla24], which is set to appear in the *International Journal of Number Theory*.

CURRICULUM VITAE

NAME OF AUTHOR: Samantha Nicole Platt

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

University of Oregon, Eugene, OR
Pittsburg State University, Pittsburg, KS
University of Ghana, Accra, Ghana
Highland Community College, Highland, KS

DEGREES AWARDED:

Doctor of Philosophy, Mathematics, 2024, University of Oregon
Master of Science, Mathematics, 2021, University of Oregon
Bachelor of Arts, Mathematics, 2017, Pittsburg State University
Bachelor of Arts, English with an Emphasis in Creative Writing in Fiction, 2017, Pittsburg State University

AREAS OF SPECIAL INTEREST:

Algebraic Number Theory
Class Field Theory
Exponential Sums
Elliptic Curves with Complex Multiplication

PROFESSIONAL EXPERIENCE:

Graduate Employee, University of Oregon, 2018-2024

GRANTS, AWARDS, AND HONORS:

Paul and Harriet Civin Memorial Graduate Student Award
E.M. Johnson Memorial Scholarship
Promising Scholar Award

ACKNOWLEDGMENTS

I would not be here nor would I have finished this work without the immense help and support of so many. First, I would like to thank my advisor, Ellen Eischen. Thank you for your guidance—both with the math itself and with how to be a mathematician—throughout my time as your student. Thank you especially for your patience and support.

Thank you as well to the rest of my committee members—Nick Addington, Ben Young, Yefeng Shen, and Woan Foong Wong—for all your time and energy. And thank you to the individuals involved with the Harriet Civin Memorial Graduate Student Award, the E.M. Johnson Memorial Scholarship, and the Promising Scholar program; these programs substantially helped me throughout my time in grad school.

I would also like to thank the many people with whom I had conversations that influenced this dissertation. Ben Young helped me see new perspectives, and his discovery-via-happy-accident led me down new research paths. My conversations with David Lowry-Duda, John Voight, and Joseph Silverman at ANTS and MSRI helped me work out some mathematical and programming kinks. Jon Aycock's excitement to talk math helped me understand many topics on a deeper level. I would also especially like to thank Greg, Francis, Jaxon, Joe, Elisa, Shabnam, and everyone else in the number theory group at Oregon. Not only were our conversations helpful, but you all created an incredibly welcoming academic community in an environment that often feels very unwelcoming.

Thank you as well to all the other friends I made at UO. Ava, Arya, Kyla, Heather, Hanna, Halley, Sarah, Jesse, Gary, and everyone with the AWM more generally—without you, my time here would have lacked so much joy and would have been decidedly more isolating. I would like to extend a special thanks to Ja-

clyn, Kelly, and Trieste, whose friendships have meant so much and without whom I probably wouldn't have stayed.

To April, Phil, and Jane, thank you for your friendship and for providing a lifeline to the world outside academia. You all also allowed me to have my many personal crises, and I greatly appreciate your patience and willingness to talk things through with me. Thank you especially to April for your help and vast expertise with coding; without you, this project would have been many, many times more painful.

Thank you to Cynthia Huffman for your time and for supporting my desire to go to grad school, and thank you to Nicoya and the rest of the Learning Commons group for your friendship, your advice, and the many hours playing Scrabble.

Finally, thank you to my family. You may not have always understood my path in life, but I am very grateful that your support has never wavered. To Grandma Shirley, I wish you could have seen me graduate, but I will always be thankful for the time I had with you and that I was lucky enough to have you as a role model. To my dad, Grandma Mary, and Aunt Cathy, thank you for always being interested in what and how I was doing. To my brothers, thank you for the constant humor—though you'll have to change up the doctor jokes now. And lastly, thank you to my mom. Thank you for always being there, for always supporting me, and for always showing me what true strength, dependability, and love both look and feel like.

Dedicated to my mom

Without you, I would never have been the person I am today.

TABLE OF CONTENTS

Chapter Page

LIST OF FIGURES

Figure Page

LIST OF TABLES

Table Page

CHAPTER 1

INTRODUCTION

The goal of this dissertation is to build on the work of Duke, Garcia, Hyde, Lutz, and many others in the study of visual aspects of Gaussian periods. In particular, we explore new visual properties of Gaussian periods, while also motivating and initiating the exploration of certain analogous constructions.

The work presented in this dissertation includes and expands upon [Pla24], which is set to appear in the *International Journal of Number Theory*.

1.1 Historical Motivation

Gaussian periods are certain exponential sums which are important in various areas of mathematics, especially number theory. Gauss originally used them when studying ruler and compass constructions and quadratic reciprocity, and they have since been used by other well-known mathematicians. For example, Kummer studied them while proving part of Fermat's Last Theorem and while investigating cyclotomic fields more generally. More recently, Lenstra and Pomerance used Gaussian periods to better optimize the AKS primality test (the first deterministic, polynomial-time primality test). Gaussian periods also have connections to Gauss sums, which show up in the functional equations of Dirichlet L-functions, among other places. For these reasons and more, Gaussian periods have been used and studied in a variety of ways throughout the years.

However, Gaussian periods were not studied *visually* until only very recently, where the increased computational capabilities of modern computers have made this possible. By plotting Gaussian periods in the complex plane, one immediately notices the many striking visual patterns which emerge.

These patterns were first discovered about a decade ago by Bob Lutz, who at the time was an undergraduate at Pomona College. Lutz had decided to experiment by creating these Gaussian period plots, and his experimentation and discoveries led to many interesting results and several papers with collaborators.

In addition to Bob Lutz, the visual study of Gaussian periods started mainly with works from Brumbaugh et al., Duke, Garcia, and Hyde [BBF$^+$14, BBGG$^+$13, DGL15, GHL15]. Their results constitute the bulk of what motivated this project, and we use a few key theorems of theirs as base points for exploration.

1.2 Structure of This Dissertation

We start in Section 1.3 by formally defining Gaussian periods and Gaussian period plots, and we use examples to showcase many of their interesting patterns. In Section 1.4, we spend some time going over some key motivational theorems from [DGL15] and providing context. We then spend the rest of this chapter explaining the two main frameworks through which we can view Gaussian periods: the framework of character theory in Section 1.5 and the framework of class field theory in Section 1.6.

However, before discussing the character theory and class field theory analogues of Gaussian periods, we focus in Chapter 2 on studying certain aspects of Gaussian periods themselves. In particular, in Section 2.1 we study the Laurent polynomials g_d which show up in Theorem 1.2, and we discuss how Gaussian periods can be viewed as traces of special unitary matrices. Additionally, we introduce a more dynamic perspective with which to study Gaussian periods in Section 2.2. We use these two perspectives to prove Proposition 2.2, which describes and explains certain dynamic behaviors of Gaussian period plots.

In Chapter 3, we explore Gaussian periods using the framework of character theory. Generally speaking, the authors mentioned above studied Gaussian period plots through the framework of supercharacter theory—a generalization of character theory which can be more conducive to computations. In Section 3.1, we discuss how Gaussian periods can be generalized using supercharacter theory, and in Definition 3.3, we explicitly define one such generalization. Using this generalization, we prove Theorem 3.4 in Section 3.2, which substantially extends a theorem of Duke, Garcia, and Lutz [DGL15, Theorem 6.3]. Additionally, in Section 3.3, we show that Theorem 3.4 cannot be generalized further without adding assumptions. We end Chapter 3 with Section 3.4, where we discuss various computational strategies that are useful when studying the objects described in this dissertation.

Although the existing literature has focused on Gaussian period plots through a supercharacter theory perspective, we can also view plots of Gaussian periods through the lens of number theory and class field theory. In particular, the well-known result of Kronecker and Weber states that every finite abelian extension of the rational numbers is contained in some cyclotomic field. Given that Gaussian periods are sums of roots of unity, one might then wonder how Gaussian periods could be generalized to other base fields, what sorts of behaviors these generalizations exhibit, and what sort of insight this study could provide.

We discuss these questions and more in Chapter 4. In particular, in Definition 4.22 of Section 4.3, we explicitly define a generalization of Gaussian periods using the class field theory of quadratic imaginary base fields. We provide the necessary background for this definition in Section 4.1, and in Section 4.2, we prove Proposition 4.20, which explicitly computes the Galois group that is needed for Definition 4.22. Once this generalization has been defined, we explore the patterns of the resulting plots in Section 4.4. In Section 4.5, however, we discuss the many compu-

tational and mathematical barriers that exist in trying to study these plots with mathematical rigor.

Finally, it is our hope that an interested reader will be inspired to investigate and experiment with these constructions on their own, and to this end we have provided a GitHub link to our code in Appendix 4.5.

Summary of Main Results

For convenience, we provide the following list of the main results and contributions presented in this dissertation.

1. Proposition 2.2 gives an explicit bound on the values of $\eta_{n,\omega}(k)$ when in the setting of Theorem 1.2.

2. Definition 3.3 defines a generalization of Gaussian periods using supercharacter theory.

3. Theorem 3.4 greatly generalizes the result of Theorem 1.2 using the supercharacter theory construction of Definition 3.3.

4. Proposition 4.20 computes the Galois group of ray class fields over Hilbert class fields when the base field is quadratic imaginary.

5. Definition 4.22 defines a generalization of Gaussian periods using the class field theory of quadratic imaginary fields, while Definition 4.24 defines this generalization for any base field.

1.3 Definitions

We begin by clarifying the definition of Gaussian periods which we will be using. Throughout this document, we define $e(x) := e^{2\pi i x}$.

Definition 1.1. Let n be an integer, and let ω be an integer coprime to n. We can identify ω as a representative of an equivalence class in $(\mathbb{Z}/n\mathbb{Z})^\times$, and we use a common abuse of terminology to say that ω is an element of $(\mathbb{Z}/n\mathbb{Z})^\times$. Let d be the multiplicative order of ω mod n; that is, d is the smallest positive integer such that $\omega^d \equiv 1 \bmod n$. For an integer k (using notation similar to [EG20]), we define the following map:

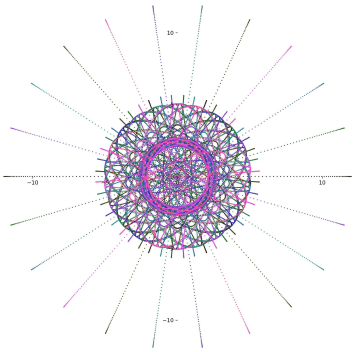
$$\eta_{n,\omega} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}, \qquad \eta_{n,\omega}(k) := \sum_{j=0}^{d-1} e\left(\frac{\omega^j k}{n}\right).$$

We call $\eta_{n,\omega}(k)$ a *Gaussian period of modulus n and generator ω* (note that we do not require k to be relatively prime to n in our definition). Additionally, we call $\mathrm{img}(\eta_{n,\omega})$ the *Gaussian period plot of modulus n and generator ω*. We use *Gaussian period* and *Gaussian period plot* when n and ω are clear from context.

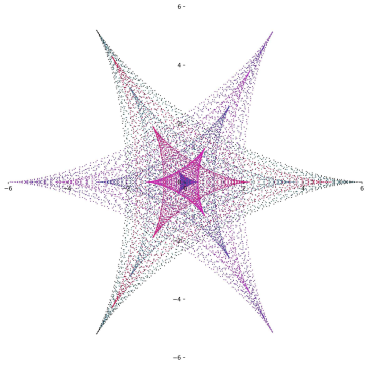
In Figure 1.1, we provide examples of Gaussian period plots for various choices of n and ω.

To clarify what's happening in this images, each dot represents the value of a single Gaussian period in the complex plane. In other words, each dot is the complex number corresponding to $\eta_{n,\omega}(k)$ for some $k \in \mathbb{Z}/n\mathbb{Z}$.

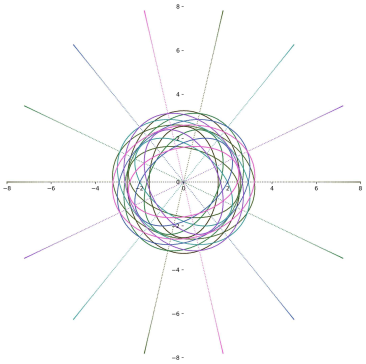
Additionally, we've colored the dots according to a "color modulus" c. The color modulus is a chosen integer less than n (usually one that divides n), and two Gaussian periods $\eta_{n,\omega}(k)$ and $\eta_{n,\omega}(k')$ are given the same color when $k \equiv k' \bmod c$. We won't focus too much on the color scheme here; as far as this document is concerned, the main benefit is that the colors help to differentiate patterns in the Gaussian period plots. For more information on the coloring scheme, we refer the reader to [EG20] and [GHL15, §3].



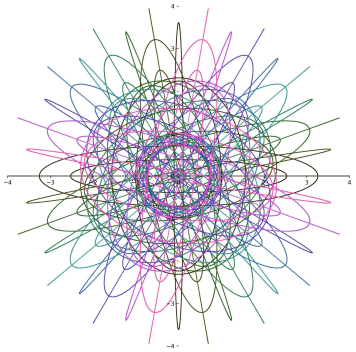
(a) $n = 255255$, $\omega = 254$, $c = 11$



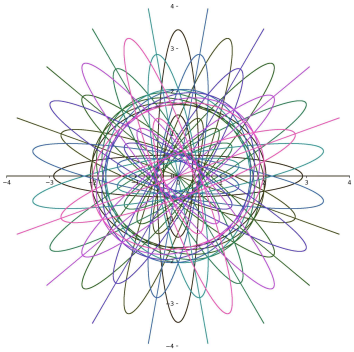
(b) $n = 82677$, $\omega = 8147$, $c = 21$



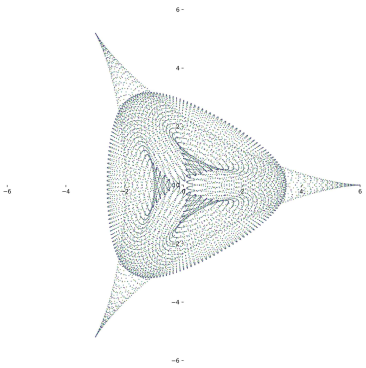
(c) $n = 70091$, $\omega = 21792$, $c = 7$



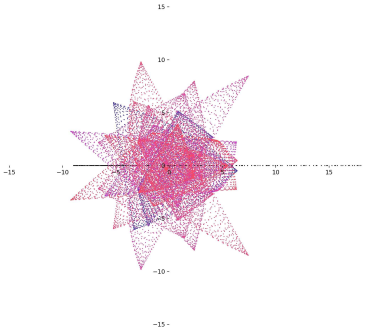
(d) $n = 455175$, $\omega = 107218$, $c = 9$



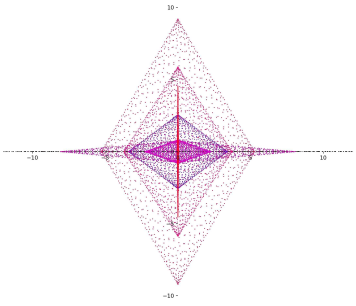
(e) $n = 478125$, $\omega = 3124$, $c = 9$



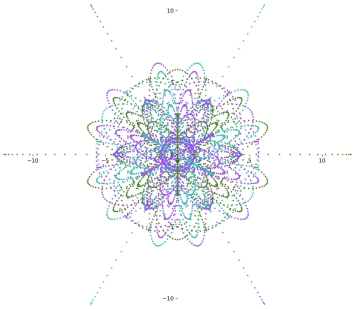
(f) $n = 52059$, $\omega = 766$, $c = 3$



(g) $n = 328549$, $\omega = 9247$, $c = 127$



(h) $n = 91205$, $\omega = 1322$, $c = 37$



(i) $n = 62160$, $\omega = 319$, $c = 3$

Figure 1.1. Examples of Gaussian period plots for various choices of n and ω

1.4 Motivational Results

Already in just the examples provided in Figure 1.1, one can see the variety of patterns that are present in Gaussian period plots. It is now that one might wonder if these patterns might be described or explained mathematically, as they obviously seem to have some sort of structure and symmetry. While there are some cases in which such a description is still unknown, there are many in which we do indeed have an explanation. In this section, we offer a few of these explanations in order to get a flavor of what has been proven thus far as well as to motivate our explorations going forward.

The first of these is a theorem of Duke, Garcia, and Lutz from [DGL15]. This theorem has been a major source of inspiration during this research project, and we spend a large part of the next two chapters exploring and expanding on certain aspects of this result. Because of this, we will often refer to this theorem as the "DGL Theorem" from here on.

Theorem 1.2 (Theorem 6.3 of [DGL15])**.** *Let $n = p^a$, where p is an odd prime. Choose $\omega \in (\mathbb{Z}/p^a\mathbb{Z})^\times$ so that its multiplicative order d divides $p-1$. Let $\Phi_d(x)$ denote the d-th cyclotomic polynomial, and let $\mathbb{T}$ denote the complex unit circle. Then the Gaussian period plot $img(\eta_{n,\omega})$ is contained in the image of the Laurent polynomial function $g_d : \mathbb{T}^{\varphi(d)} \to \mathbb{C}$ defined by*

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

where the constants c_{mj} are defined by the following relations:

$$x^j \equiv \sum_{m=0}^{\varphi(d)-1} c_{mj} x^m \ mod\ \Phi_d(x).$$

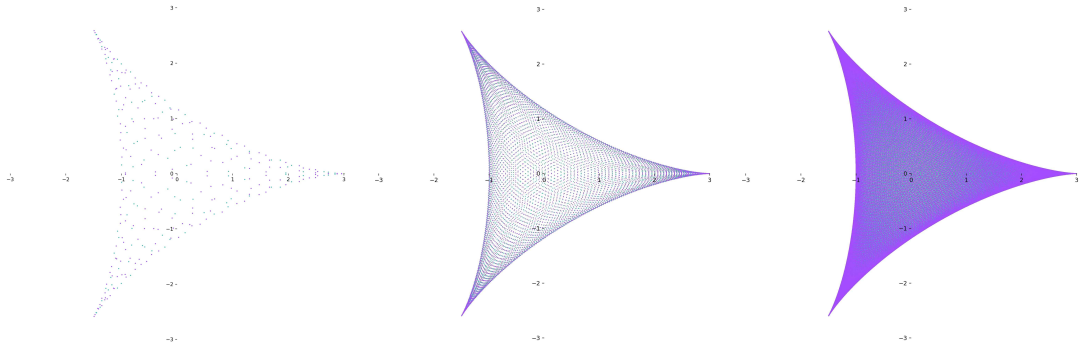
Moreover, for a fixed d, as p^a tends to infinity (where the prime $p \equiv 1$ mod d, the power a, and the choice of ω are allowed to vary), every nonempty open disc contained in $\text{img}(g_d)$ eventually contains points in $\text{img}(\eta_{n,\omega})$. In other words, $\text{img}(g_d)$ is "filled out" by Gaussian periods as n goes to infinity.

We provide examples of Theorem 1.2 in Figure 1.2.

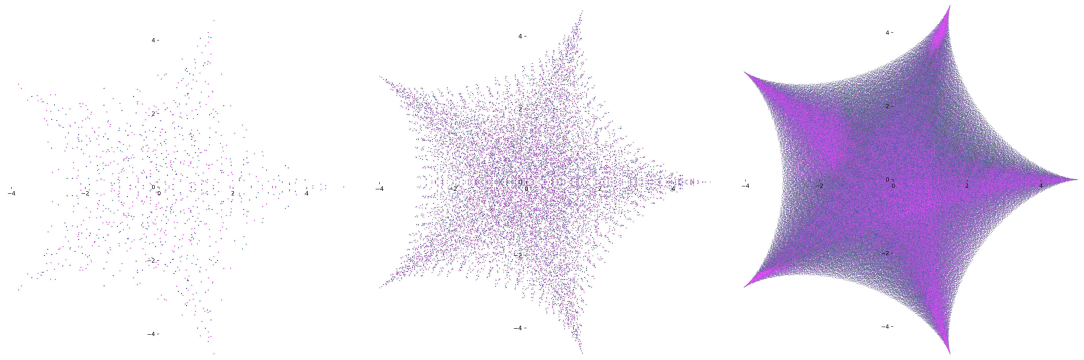
The Laurent polynomials g_d showing up in the DGL Theorem are interesting objects of study in their own right. They depend only on the integer d, and they are defined via some polynomial modular arithmetic using the cyclotomic polynomials Φ_d. Given the variety of well-known properties about cyclotomic polynomials, it might not be surprising to learn that g_d has some interesting properties as well. In Section 2.1, we spend some time studying these Laurent polynomials, and we use some of their properties to prove some results about Gaussian period plots. Additionally, in Table 2.1, we provide examples of g_d for small d.

For now, it is of particular interest to note that in the case where d is itself also a prime, the image of g_d is a *d-sided hypocycloid*. A hypocycloid is a shape cut out in the plane by taking two circles, fixing a point on the smaller circle, and then tracing that fixed point as the smaller circle rolls along the inside of the larger one. Examples of these shapes can be found in images (a) through (d) of Figure 1.2.

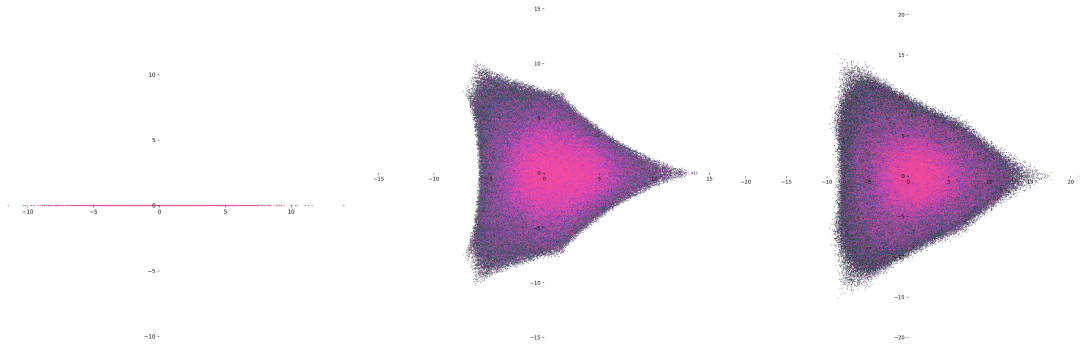
Finally, we note that the DGL Theorem has been reinterpreted by Untrau and Kowalski in [Unt24, KU23] as a statement about the distribution of points in the complex plane under the pushforward measure of the Haar measure on $\mathbb{T}^{\varphi(d)}$ via the map g_d. Untrau and Kowalski then use this reinterpretation as a starting point from which they generalize to other situations. While this perspective is not the focus of this dissertation, the relationship to the distribution of points in the complex plane will show up again in Remarks 3.10 and 3.12 relating to Theorem 3.4.



(a) $n = 31^2$, $\omega = 521$, $d = 3$ *(b)* $n = 31^3$, $\omega = 23503$, $d = 3$ *(c)* $n = 13^5$, $\omega = 220860$, $d = 3$



(d) $n = 71^2$, $\omega = 2752$, $d = 5$ *(e)* $n = 41^3$, $\omega = 46244$, $d = 5$ *(f)* $n = 41^4$, $\omega = 629614$, $d = 5$



(g) $n = 29^3$, $\omega = 22517$, $d = 14$ *(h)* $n = 31^5$, $\omega = 17404906$, $d = 15$ *(i)* $n = 43^5$, $\omega = 67107967$, $d = 21$

Figure 1.2. Examples of Duke–Garcia–Lutz Theorem for various values of d

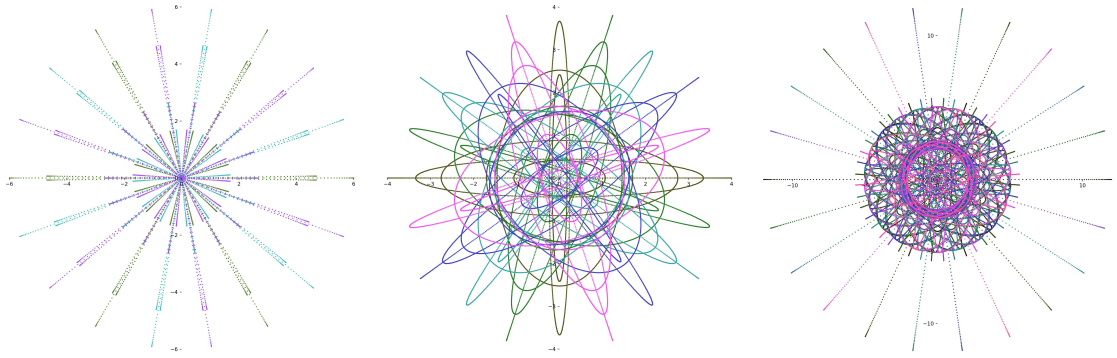
While the DGL Theorem provides inspiration and several avenues of exploration, there is one other previous result that we will highlight here. We've chosen this one because it offers some insight into other sorts of structures that are contained in Gaussian period plots.

Before stating this result, however, we need a quick definition.

Definition 1.3. The Gaussian period plot $\mathrm{img}(\eta_{n,\omega})$ is said to have *m-fold dihedral symmetry* if it is invariant under the natural action of the dihedral group of order $2m$. In other words, $\mathrm{img}(\eta_{n,\omega})$ has m-fold dihedral symmetry if it is invariant under complex conjugation and rotation by $2\pi/m$ about the origin.

Proposition 1.4 (Prop. 3.1 of [DGL15])**.** *Let n, ω, and d be as in Definition 1.1. Let $m = \gcd(\omega - 1, n)$. Then the Gaussian period plot $img(\eta_{n,\omega})$ has m-fold dihedral symmetry.*

We provide examples of this m-fold dihedral symmetry in Figure 1.3.



(a) $n = 29070$, $\omega = 1189$, $d = 6$, $m = 18$ *(b)* $n = 91205$, $\omega = 39626$, $d = 4$, $m = 5$ *(c)* $n = 255255$, $\omega = 254$, $d = 12$, $m = 11$

Figure 1.3. Examples of Gaussian period plots with m-fold dihedral symmetry

1.5 Character Theory

Now that we have an idea of some of the properties of Gaussian period plots, we return to discussing the two main frameworks through which we can view Gaussian periods. These two frameworks will form the basis of our discussions in Chapters 3 and 4, and we will use these two perspectives to generalize the construction of Gaussian periods to other situations.

The first of these frameworks is character theory, which—as mentioned at the beginning of the chapter—is the framework through which a majority of the previously mentioned authors have studied Gaussian period plots. In particular, they used a generalization of character theory known as *supercharacter theory*.

Supercharacter theory was first described axiomatically for finite groups by Diaconis and Isaacs in 2008 [DI08], building on the work of André in his study of the representation theory of unipotent matrix groups [And01, And95]. More recently in 2021, André and Lochon have extended this definition to countable discrete groups [AL21].

As mentioned in [GHL15, §3], supercharacter theory has been used in the study of a variety of objects, including the Hopf algebra of symmetric functions of noncommuting variables [AAB$^+$12], random walks on upper triangular matrices [ACDS04], combinatorial properties of Schur rings [DT09, Thi10, TV09], and Ramanujan sums [FGK14].

Since we will be concerned primarily with finite groups, we use the definition of Diaconis and Isaacs.

Definition 1.5. Let G be a finite group with identity 1, let $\mathcal{K}$ be a partition of G, and let $\mathcal{X}$ be a partition of the set of irreducible characters of G. Then $(\mathcal{X}, \mathcal{K})$ is a *supercharacter theory* for G if the following hold:

- $\{1\} \in \mathcal{K}$
- $|\mathcal{X}| = |\mathcal{K}|$
- For each $X \in \mathcal{X}$, the function $\sigma_X = \sum_{\chi \in X} \chi(1)\chi$ is constant on each $K \in \mathcal{K}$.

The elements $K \in \mathcal{K}$ are called *superclasses*, and the functions σ_X are called *supercharacters*.

Using the above definition, let $G = \mathbb{Z}/n\mathbb{Z}$. For every $x \in G$, there exists an irreducible character χ_x such that

$$\chi_x : G \to \mathbb{C}, \qquad \chi_x(y) = e\left(\frac{xy}{n}\right).$$

In fact, the characters χ_x describe all of the irreducible characters of G. For the cyclic subgroup $\langle \omega \rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$, let $\mathcal{K}$ be the partition of G corresponding to the orbits of the action $a \cdot x = ax$ for $a \in \langle \omega \rangle$. Additionally, let $\mathcal{X}$ be the partition of the irreducible characters of G corresponding to the action $a \cdot \chi_x = \chi_{a^{-1}x}$. One can then check that $\mathcal{X}$ and $\mathcal{K}$ are compatible as in the definition given above (in fact, in Proposition 3.1, we will prove that a more general construction satisfies this definition). Thus $(\mathcal{X}, \mathcal{K})$ defines a supercharacter theory on $\mathbb{Z}/n\mathbb{Z}$, and the supercharacter $\sigma_{\langle \omega \rangle}$ corresponding to the orbit of $1 \in G$ is precisely the map $\eta_{n,\omega}$ from Definition 1.1.

With this perspective in mind, the DGL Theorem, for example, gives a geometric description of the values which show up in a "supercharacter table" for $(\mathcal{X}, \mathcal{K})$ when $n = p^a$ is the power of an odd prime and ω has order $d \mid (p-1)$. Additionally, Proposition 1.4 describes certain symmetries in a supercharacter table.

To end this section, we include a brief remark on the choice of subgroup $\langle \omega \rangle$.

Remark 1.6. It should be noted that the above construction of the partitions $\mathcal{X}$ and $\mathcal{K}$ work for *any* subgroup $\Gamma \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$ and not just the cyclic subgroups that we chose. As long as one is careful in defining the Γ-action on G and its characters, the induced partitions will always give a supercharacter theory. This is a result from [BBF$^+$14, §1], which we record later as Proposition 3.1. For our purposes, however, we mainly restrict ourselves to the case in which Γ is cyclic, though we do believe it is worth exploring supercharacter theories induced by non-cyclic subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$.

1.6 Class Field Theory

The second framework through which to view Gaussian periods is class field theory. Before discussing this framework, we include a short remark on the limitations of our treatment of this subject.

Remark 1.7. We note that we will not be describing general class field theory in great detail, as we will be providing only a general overview for motivation. Because of this, it isn't expected that the reader know these details in order to understand any results; however, some discussions (the proof for Proposition 4.20 in particular) may be difficult to follow without much background. For further reading about class field theory, we recommend [Chi09, CS08, Cox13].

Now, given a base field K, the main goal of class field theory is to describe all finite abelian extensions of K (i.e. extensions L/K such that $\mathrm{Gal}(L/K)$ is a finite abelian group), and it aims to do so using the local properties of K (i.e. the set of primes or "places" of K). In most cases, class field theory allows us to compute the Galois groups of these field extensions fairly easily. However, explicitly finding the fields corresponding to such Galois groups is often a much harder task. In fact,

this is the subject of Hilbert's 12th problem, which is concerned with determining which algebraic numbers must be adjoined to K in order to generate its abelian extensions.

The answer to Hilbert's 12th problem is known in very few cases. The first of these is the one in which $K = \mathbb{Q}$. In this case, the Kronecker-Weber Theorem states that every finite abelian extension of $\mathbb{Q}$ is contained in some finite cyclotomic extension of $\mathbb{Q}$. That is, the abelian extensions of $\mathbb{Q}$ are generated by roots of unity.

Another case in which the answer is known (and which is a source of exploration in Chapter 4) is the case in which K is a quadratic imaginary field—i.e. $K = \sqrt{-D}$ for some positive squarefree integer D. In this case, the well-known theory of complex multiplication gives us our answer: all finite abelian extensions of K are generated by adjoining certain values of the modular j-function along with coordinates of torsion points of elliptic curves with complex multiplication by $\mathcal{O}_K$. A more in-depth description and explanation of this is provided in Section 4.1.

The last major case in which Hilbert's 12th problem has been answered is the case in which K is a totally real field—i.e. in which the image of every embedding $\sigma : K \hookrightarrow \mathbb{C}$ is contained in the real numbers. In this case, abelian extensions of K are generated by adjoining certain square roots of elements of K along with Brumer-Stark units, which are elements constructed using p-adic integration. This result was proven by Dasgupta and Kakde only very recently in [DK23]. While we won't be using their result in this dissertation, it is still worth mentioning.

With these examples in mind, we offer the following definitions from class field theory.

Definition 1.8. Let K be a number field, and let $\mathcal{O}_K$ be its ring of integers. Given

an ideal $\mathfrak{m} \subseteq \mathcal{O}_K$ called the *modulus*, we obtain a *ray class group of modulus* $\mathfrak{m}$, which we denote by $Cl_K(\mathfrak{m})$. For each ray class group of modulus $\mathfrak{m}$, there exists a *ray class field of modulus* $\mathfrak{m}$, denoted by $K[\mathfrak{m}]$, whose Galois group $\mathrm{Gal}(K[\mathfrak{m}]/K)$ is isomorphic to $Cl_K(\mathfrak{m})$ and whose set of ramified primes are only those which divide $\mathfrak{m}$. In the special case where $\mathfrak{m} = (1)$, we call $K[1]$ the *Hilbert class field*, whose Galois group $\mathrm{Gal}(K[1]/K)$ is isomorphic to the ideal class group $Cl_K(1)$ of K.

In addition to the above definitions, we make two important notes about ray class groups and ray class fields. First, if $\mathfrak{n}$ is an ideal dividing $\mathfrak{m}$, then $Cl_K(\mathfrak{n}) \subseteq Cl_K(\mathfrak{m})$ and $K[\mathfrak{n}] \subseteq K[\mathfrak{m}]$. One important implication of this is that the Hilbert class field is an intermediate field extension for every modulus $\mathfrak{m}$; that is, $K \subseteq K[1] \subseteq K[\mathfrak{m}]$ for every $\mathfrak{m}$.

Additionally, we note that there is an alternate description of ray class fields. Rather than viewing them through the correspondence provided above, one can instead define ray class fields of modulus $\mathfrak{m}$ to be the maximal abelian extension of K which is ramified only at the primes dividing $\mathfrak{m}$, assuming a certain boundedness condition related to $\mathfrak{m}$. These two characterizations turn out to be equivalent, and we will be using them interchangeably in our discussion.

We summarize the above definitions and comments in the following diagram of field extensions and Galois groups.

$$\begin{array}{l} K[\mathfrak{m}] \\ \quad \Big| \ \mathrm{Gal}(K[\mathfrak{m}]/K[1]) \\ Cl_K(\mathfrak{m}) \quad K[1] \\ \quad \Big| \ Cl_K(1) \\ K \end{array}$$

Example 1.9. In the case where $K = \mathbb{Q}$, the ring of integers is $\mathbb{Z}$. The ideal

class group of $\mathbb{Q}$ is trivial, so the Hilbert class field is $\mathbb{Q}$ itself. Also, given an ideal $(m) \subseteq \mathbb{Z}$, the ray class group of modulus m is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$, and the corresponding ray class field is $\mathbb{Q}(\mu_m)$, where $\mu_m \subseteq \mathbb{C}^\times$ denotes the subgroup of m-th roots of unity.

Returning to the discussion of Gaussian periods, note that $e\left(\frac{k}{n}\right)$ is an n-th root of unity for every integer k. Thus every summand in $\eta_{n,\omega}(k)$ sits inside the n-th cyclotomic field $\mathbb{Q}[n] = \mathbb{Q}(\mu_n)$. Since ω is assumed to be an element of $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}[n]/\mathbb{Q})$, the Gaussian periods of modulus n and generator ω are sums over the Galois action of the cyclic subgroup $\langle\omega\rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$. In particular, this implies that $\eta_{n,\omega}(k)$ is an element of $\mathbb{Q}[n]^{\langle\omega\rangle}$, the subfield of $\mathbb{Q}[n]$ fixed by the action of $\langle\omega\rangle$.

In fact, Gaussian periods are not only *contained* in subfields of ray class fields, but they are *generators* of those subfields. These subfields are important objects of study in number theory, as they are abelian extensions of $\mathbb{Q}$ ramified only at the primes dividing the modulus of the ray class field; they just aren't the maximal such extension.

With this perspective in mind, we see that the DGL Theorem shows how these generators are distributed in $\mathbb{C}$, as well as a description of their asymptotic behavior. Additionally, Propositions 1.4 further describe the distribution of these points.

We have now seen the definition of Gaussian periods and Gaussian period plots, some key results pertaining to them, and two main frameworks through which to understand them. Before discussing generalizations of Gaussian periods in Chapters 3 and 4, we discuss a new way to study Gaussian periods and we prove further properties of Gaussian period plots and some objects related to them.

CHAPTER 2

DYNAMIC PROPERTIES OF GAUSSIAN PERIODS

The work presented in this chapter includes and expands upon [Pla24, §3], which is set to appear in the *International Journal of Number Theory*.

In this chapter, we explore various aspects of the DGL Theorem. In particular, we start with a more in-depth discussion of the Laurent polynomials g_d, and then we introduce a new, dynamic perspective on Gaussian periods, culminating in an explicit boundedness result in Proposition 2.2.

We recommend that the reader review the DGL Theorem from Chapter 1, as we will be referring to it throughout this chapter.

2.1 The Laurent Polynomials g_d

We start by looking at the Laurent polynomials g_d in more detail. Given a positive integer d, recall that we have the following definition:

$$g_d : \mathbb{T}^{\varphi(d)} \to \mathbb{C}, \qquad g_d(z_1, z_2, \ldots, z_{\varphi(d)}) = \sum_{j=0}^{d-1} \prod_{m=0}^{\varphi(d)-1} z_{m+1}^{c_{mj}},$$

where the constants c_{mj} are defined by the relations

$$x^j \equiv \sum_{m=0}^{\varphi(d)-1} c_{mj} x^m \bmod \Phi_d(x),$$

where $\Phi_d(x)$ is the d-th cyclotomic polynomial. As we will see in the proof of Theorem 3.4, this definition of g_d arises naturally when studying Gaussian periods, and in fact, we discuss a natural generalized construction of similar Laurent polynomials in Section 3.3.

It turns out that the image of g_d is sometimes more or sometimes less interesting for various values of d. For example, if d is even, then $\mathrm{img}(g_d)$ is totally real.

This makes sense if we realize what this means in the context of the DGL Theorem. Since $n = p^a$ is a power of an odd prime, then note that $(\mathbb{Z}/p^a\mathbb{Z})^\times$ is a cyclic group. If d is divisible by 2, then $\langle\omega\rangle$ must contain -1, which is the only element of order 2. If $\langle\omega\rangle$ contains -1, then we must have that $\overline{\eta_{n,\omega}(k)} = \eta_{n,\omega}(k)$ for all k, which implies that $\text{img}(\eta_{n,\omega})$ is entirely real.

However, note that if d is a prime, then $\varphi(d) = d-1$ and $\Phi_d(x) = x^{d-1} + x^{d-2} + \cdots + 1$. Thus we have the following:

$$x^j \equiv \begin{cases} x^j \bmod \Phi_d(x) & 0 \leq j < d-1, \\ (-x^{d-2} - \cdots - x - 1) \bmod \Phi_d(x) & j = d-1. \end{cases}$$

Thus when d is prime, we get

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

Since each z_i is on the unit circle, it is easy to check that the boundary of $\text{img}(g_d)$ is cut out by the image of the diagonal $z_1 = z_2 = \cdots = z_{d-1}$. If we write $z_i = e^{i\theta}$ for some $\theta \in [0, 2\pi)$, then we see that the boundary of $\text{img}(g_d)$ is given by

$$(d-1)e^{i\theta} + e^{-i(d-1)\theta}.$$

The image cut out by this function as θ varies across $[0, 2\pi)$ is precisely a d-sided hypocycloid, as we see in Figure 1.2.

Additionally, if $d = q^b$ is a power of an odd prime, then Garcia, Hyde, and Lutz proved the following result.

Proposition 2.1 (Corollary 1 of [GHL15]). *If $d = q^b$ is a power of an odd prime, then the image of g_{q^b} is the Minkowski sum*

$$\sum_{j=1}^{q^{b-1}} H_q,$$

where H_q is the filled-out q-sided hypocycloid and the Minkowski sum of two nonempty sets $S, T \subseteq \mathbb{C}$ is defined to be

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

In other words, when $d = q^b$ is a power of an odd prime, the image of g_d is simply sums of copies of $\text{img}(g_q)$.

The most interesting case—and the one that remains unexplained—is the one in which d is a product of distinct odd primes. One can see examples of this when $d = 15$ in Figure 1.2h and when $d = 21$ in Figure 1.2i. This author, among several others, has been unable to correctly identify the shapes which arise in these situations, and thus there has yet to be an analogous explanation of the geometry of $\text{img}(g_d)$.

Now, it may be of interest to the reader to explicitly generate examples of g_d for themselves. To this end, we included a link in Appendix 4.5 to the code we used for this project. In the SageMath files, one will find the function DGLLaurentPoly(d), which will automatically generate the formula for g_d given a positive integer d. The function LatexDGLLaurentPoly(d) computes the same polynomial, but writes it into LaTeX-friendly code.

We end this section with Table 2.1, which contains a handful of Laurent polynomials g_d when d is small and non-prime. The entries in this table were generated using the code mentioned above.

2.2 Animations of Gaussian Periods

Using our knowledge of the polynomials $g_d(z_1, \ldots, z_{\varphi(d)})$, we now explore some observations made by the Duke, Hyde, and Lutz in sections 5 and 6 of [GHL15].

$$
\begin{aligned}
g_4(z_1,z_2) &= z_1+z_2+\frac{1}{z_1}+\frac{1}{z_2}\\
g_6(z_1,z_2) &= z_1+z_2+\frac{1}{z_1}+\frac{1}{z_2}+\frac{z_1}{z_2}+\frac{z_2}{z_1}\\
g_8(z_1,z_2,z_3,z_4) &= z_1+z_2+z_3+z_4+\frac{1}{z_1}+\frac{1}{z_2}+\frac{1}{z_3}+\frac{1}{z_4}\\
g_9(z_1,\ldots,z_6) &= z_1+z_2+z_3+z_4+z_5+z_6+\frac{1}{z_1z_4}+\frac{1}{z_2z_5}+\frac{1}{z_3z_6}\\
g_{10}(z_1,z_2,z_3,z_4) &= z_1+z_2+z_3+z_4+\frac{z_1z_3}{z_2z_4}+\frac{z_2z_4}{z_1z_3}+\frac{1}{z_1}+\frac{1}{z_2}+\frac{1}{z_3}+\frac{1}{z_4}\\
g_{12}(z_1,\ldots,z_4) &= z_1+z_2+z_3+z_4+\frac{z_1}{z_3}+\frac{z_3}{z_1}+\frac{z_2}{z_4}+\frac{z_4}{z_2}+\frac{1}{z_1}+\frac{1}{z_2}+\frac{1}{z_3}+\frac{1}{z_4}\\
g_{14}(z_1,\ldots,z_6) &= z_1+z_2+z_3+z_4+z_5+z_6+\frac{z_1z_3z_5}{z_2z_4z_6}+\frac{z_2z_4z_6}{z_1z_3z_5}\\
&\quad+\frac{1}{z_1}+\frac{1}{z_2}+\frac{1}{z_3}+\frac{1}{z_4}+\frac{1}{z_5}+\frac{1}{z_6}\\
g_{15}(z_1,\ldots,z_8) &= z_1+z_2+z_3+z_4+z_5+z_6+z_7+z_8\\
&\quad+\frac{z_1z_4z_7}{z_3z_5z_8}+\frac{z_2z_5z_8}{z_1z_4z_6}+\frac{z_1z_6}{z_2z_5z_8}+\frac{z_3z_8}{z_1z_4z_7}+\frac{1}{z_1z_6}+\frac{1}{z_2z_7}+\frac{1}{z_3z_8}\\
g_{21}(z_1,\ldots,z_{12}) &= z_1+z_2+z_3+z_4+z_5+z_6+z_7+z_8+z_9+z_{10}+z_{11}+z_{12}\\
&\quad+\frac{z_1z_4z_8z_{11}}{z_3z_6z_9z_{12}}+\frac{z_2z_5z_9z_{12}}{z_1z_4z_7z_{10}}+\frac{z_1z_4z_7z_{10}}{z_2z_5z_6z_9z_{12}}+\frac{z_3z_6z_9z_{12}}{z_1z_4z_7z_8z_{11}}\\
&\quad+\frac{1}{z_1z_8}+\frac{1}{z_2z_9}+\frac{1}{z_3z_{10}}+\frac{1}{z_4z_{11}}+\frac{1}{z_5z_{12}}
\end{aligned}
$$

Table 2.1. Examples of Laurent polynomials g_d from the DGL Theorem

In particular, they make an observation about elements in the image of g_d when d is prime. We discussed above that

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

in this case. Now, because each z_i is an element of $\mathbb{T}$ (i.e. a complex number on the unit circle), we can view the sum on the right-hand side as being the trace of some $d\times d$ special unitary matrix. This is because of the following properties of special

unitary matrices.

Let $\mathrm{SU}(d)$ be the group of $d \times d$ special unitary matrices. For $U \in \mathrm{SU}(d)$, let $\{\lambda_1, \ldots, \lambda_d\}$ be the set of eigenvalues for U. Because U is unitary (i.e. $UU^* = I$, where U^* is the conjugate transpose of U), the eigenvalues λ_i are all on the unit circle. Additionally, because $\det(U) = 1$, then we have the restriction that

$$\lambda_d = \frac{1}{\prod_{i=1}^{d-1} \lambda_i}.$$

Since the trace of a matrix is the sum of its eigenvalues, then we see that the trace of $U \in \mathrm{SU}(d)$ is of the form given by elements in the image of g_d.

We now reinterpret the statement of the DGL Theorem using this perspective. Let n and ω of order d be chosen with the properties as stated in the theorem. Then the theorem states that $\eta_{n,\omega}(k) \in \mathrm{img}(g_d)$ for every $k \in \mathbb{Z}/n\mathbb{Z}$, and thus there exists some special unitary matrix $U_{n,\omega,k} \in \mathrm{SU}(d)$ such that $\eta_{n,\omega}(k) = \mathrm{Tr}(U_{n,\omega,k})$. Additionally, the "filling out" statement from the DGL Theorem implies that for any $U \in \mathrm{SU}(d)$, there exists some n, some ω of order d, and some $k \in \mathbb{Z}/n\mathbb{Z}$ such that $\eta_{n,\omega}(k)$ is arbitrarily close to $\mathrm{Tr}(U)$.

There is, in fact, a little more to this story. In writing the code needed for plotting Gaussian periods, it seems that everyone (including this author) decided simply to plot $\mathrm{img}(\eta_{n,\omega})$ all at once. That is, given an n and ω, most algorithms that were written would compute all of the Gaussian periods, plot them all at once, and then return the resulting image. However, if we instead plot Gaussian periods in *batches*, we can create an "animation" of Gaussian periods which is able to reveal more about the underlying mathematics. In the following paragraph, we discuss how these animations are created.

Assume we have a modulus n and element $\omega \in (\mathbb{Z}/n\mathbb{Z})^\times$ of order d. We then choose a constant C that is small relative to n (the author recommends $C \approx \sqrt{n}$,

though sometimes the behavior is more clear with smaller or larger C). Each additional frame of the animation will hold approximately C new Gaussian periods, resulting in $\lceil n/C \rceil$ total frames. That is, the f-th frame will be the plotted image of $\eta_{n,\omega}(k)$ for all $0 \leq k < fC$. When we string these frames together, we get an animation showing the behavior of Gaussian periods as they fill out the Gaussian period plot $\text{img}(\eta_{n,\omega})$.

The idea of creating these animations came from a happy coding mishap by Benjamin Young, in which he accidentally plotted $\eta_{n,\omega}(k)$ for only small values of k. In doing so, he discovered some unnoticed and unexplained structures of $\text{img}(\eta_{n,\omega})$, and this discovery eventually led this author to the following proposition.

Proposition 2.2 (Proposition 8 of [Pla24])**.** *Let $n = p^a$ be a power of a prime, let d be a prime dividing $p-1$, and let $\omega \in (\mathbb{Z}/n\mathbb{Z})^\times$ be an element of order d. Let $k \in \mathbb{Z}/n\mathbb{Z}$. Then the value of the k-th Gaussian period of modulus n and generator ω is contained in a $(d-1)$-sided hypocycloid centered at $e\left(\frac{k}{n}\right)$ and rotated by a factor of $e\left(\frac{-k}{(d-1)n}\right)$. That is,*

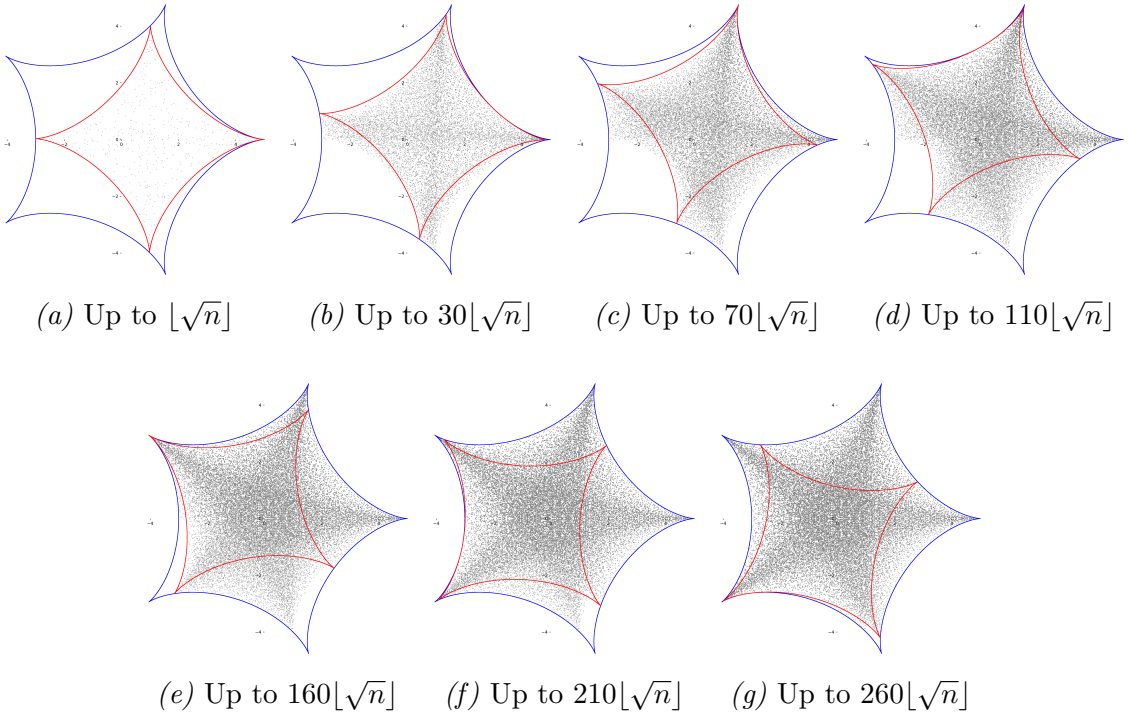
$$\eta_{n,\omega}(k) \in \left\{ e\left(\frac{k}{n}\right) + h \cdot e\left(\frac{-k}{(d-1)n}\right) \ : \ h \in H_{d-1} \right\},$$

where H_{d-1} represents the filled-in $(d-1)$-sided hypocycloid centered at the origin in the complex plane.

To explain this proposition in a different way, note that the assumptions on n, d, and ω imply that $\eta_{n,\omega}(k)$ is contained in a d-sided hypocycloid. This proposition then says that the value of $\eta_{n,\omega}(k)$ is contained within a $(d-1)$-sided hypocycloid which has been translated and rotated by a certain amount. Specifically, the $(d-1)$-sided hypocycloid has been translated and rotated in such a way that, as k goes

from 0 to $n-1$, it ends up rolling smoothly counterclockwise along the interior of the d-sided hypocycloid.

For example, if $d = 3$, then a 2-sided hypocyloid (i.e. a straight line) rolls along the inside of a 3-sided hypocycloid. When $d = 5$, a 4-sided hypocycloid rolls along the inside of a 5-sided hypocycloid. This behavior becomes quite clear in the animations of Gaussian periods mentioned above, and we include some still frames of these animations in Figure 2.1.



(a) Up to $\lfloor\sqrt{n}\rfloor$ *(b)* Up to $30\lfloor\sqrt{n}\rfloor$ *(c)* Up to $70\lfloor\sqrt{n}\rfloor$ *(d)* Up to $110\lfloor\sqrt{n}\rfloor$

(e) Up to $160\lfloor\sqrt{n}\rfloor$ *(f)* Up to $210\lfloor\sqrt{n}\rfloor$ *(g)* Up to $260\lfloor\sqrt{n}\rfloor$

Figure 2.1. A 4-sided hypocycloid rolling along the inside of a 5-sided hypocycloid when $n = 11^5$ and $\omega = 37107$

We now prove Proposition 2.2, and we do so by returning to our discussion of viewing elements of $\mathrm{img}(g_d)$ as traces of special unitary matrices.

Proof. We begin by defining the following general homomorphism, which will aid us

in the proof itself:

$$\psi_m : \mathrm{U}(1) \times \mathrm{SU}(m-1) \hookrightarrow \mathrm{SU}(m), \qquad (e^{i\theta}, U) \mapsto \mathrm{diag}(e^{i(m-1)\theta}, e^{-i\theta}U),$$

where $\mathrm{diag}(e^{i(m-1)\theta}, e^{-i\theta}U)$ represents the block-diagonal matrix with the 1×1 block $e^{i(m-1)\theta}$ and the $(m-1)\times(m-1)$ block $e^{-i\theta}U$. Composing this homomorphism with the trace map, we see that

$$\mathrm{Tr}(\psi_m(e^{i\theta}, U)) = e^{i(m-1)\theta} + e^{-i\theta}\mathrm{Tr}(U).$$

Since $U \in \mathrm{SU}(m-1)$, then $\mathrm{Tr}(U)$ is contained in the $(m-1)$-sided hypocycloid (as discussed at the beginning of this section). Additionally, note that as θ goes from 0 to 2π, the term $e^{i(m-1)\theta}$ moves counterclockwise on the unit circle and the multiplicative factor $e^{-i\theta}$ causes $\mathrm{Tr}(U)$ to rotate clockwise. Thus, if we allow $U \in \mathrm{SU}(m-1)$ to vary and we have θ increase from 0 to 2π, the result is a filled-in $(m-1)$-sided hypocycloid rolling counterclockwise along the interior of an m-sided hypocycloid.

The relationship between this homomorphism and the statement of the proposition is simple enough to see. For a given prime power n, a prime d, an $\omega \in (\mathbb{Z}/n\mathbb{Z})^\times$ of order d, and $k \in (\mathbb{Z}/n\mathbb{Z})$, recall the definition of a Gaussian period:

$$\eta_{n,\omega}(k) = e^{\frac{2\pi i k}{n}} + e^{\frac{2\pi i \omega k}{n}} + \cdots + e^{\frac{2\pi i \omega^{d-1} k}{n}}.$$

If we let $\theta = \frac{2\pi k}{(d-1)n}$, then we have the following:

$$\eta_{n,\omega}(k) = e^{i(d-1)\theta} + e^{-i\theta}\left(e^{i\theta((d-1)\omega+1)} + \cdots + e^{i\theta((d-1)\omega^{d-1}+1)}\right).$$

We will verify below that

$$\prod_{j=1}^{d-1} e^{i\theta((d-1)\omega^j+1)} = 1,$$

but for now we assume this equality is true. This then shows that

$$\left\{e^{i\theta((d-1)\omega+1)}, \ldots, e^{i\theta((d-1)\omega^{d-1}+1)}\right\}$$

are the eigenvalues of some matrix $U'_{n,\omega,k} \in \mathrm{SU}(d-1)$. Thus

$$\eta_{n,\omega}(k) = e^{i(d-1)\theta} + e^{-i\theta}\mathrm{Tr}(U'_{n,\omega,k}),$$

which shows that

$$\eta_{n,\omega}(k) = \mathrm{Tr}(\psi_d(e^{i\theta}, U'_{n,\omega,k})).$$

That is, we have shown that $\eta_{n,\omega}(k)$ is the trace of some matrix in $\mathrm{img}(\psi_d)$. Since $\mathrm{Tr}(U) \in H_{d-1}$ for any $U \in \mathrm{SU}(d-1)$, then we have that

$$\eta_{n,\omega}(k) = e\left(\frac{k}{n}\right) + h \cdot e\left(\frac{-k}{(d-1)n}\right)$$

for some $h \in H_{d-1}$ as desired. Additionally, note that $\theta = \frac{2\pi ik}{(d-1)n}$ increases as k increases, which explains the smooth rolling behavior of the $(d-1)$-sided hypocycloid along the inner boundary of the d-sided hypocycloid.

We now return to showing that

$$\prod_{j=1}^{d-1} e^{i\theta((d-1)\omega^j+1)} = 1.$$

First, note that

$$\prod_{j=1}^{d-1} e^{i\theta((d-1)\omega^j+1)} = \exp\left(i\theta \sum_{j=1}^{d-1}((d-1)\omega^j + 1)\right).$$

Expanding the sum, we get the following:

$$\begin{aligned}\sum_{j=1}^{d-1}((d-1)\omega^j + 1) &= (d-1)(\omega + \omega^2 + \cdots + \omega^{d-1}) + (d-1) \\ &= (d-1)(1 + \omega + \omega^2 + \cdots + \omega^{d-1}).\end{aligned}$$

Note that the factor of $(d-1)$ cancels the $(d-1)$ in the denominator of θ. Also, since $\omega \in (\mathbb{Z}/n\mathbb{Z})^\times$ has order d, then ω satisfies the equation $\Phi_d(\omega) \equiv 0 \bmod n$, where Φ_d is the d-th cyclotomic polynomial (for more explanation, see Remark 3.5). Since d is prime, then this implies that

$$\Phi_d(\omega) = 1 + \omega + \cdots + \omega^{d-1} \equiv 0 \bmod n.$$

Since n is the only term in the denominator of θ after canceling the $(d-1)$, then we have that

$$\prod_{j=1}^{d-1} e^{i\theta((d-1)\omega^j+1)} = e^{2\pi i m}$$

for some integer m. Thus

$$\prod_{j=1}^{d-1} e^{i\theta((d-1)\omega^j+1)} = 1,$$

which concludes our proof. □

One might now wonder what occurs in the case where d is not itself prime. Unfortunately, the geometrical shapes that one gets are much harder to describe succinctly, though the general behavior of "a smaller shape rolling counterclockwise along the boundary" seems to hold based on experimentation. But again, describing the "smaller shape" remains as elusive as describing the overall shape of the Gaussian period plots in these cases.

Regardless, note that the behavior described in Proposition 2.2 is explained in the proof using the homomorphisms ψ_d. In the following remark, we discuss the most basic version of a similar homomorphism for any d.

Remark 2.3. For any positive integer d, we have the Laurent polynomial

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

where the constants c_{mj} are defined by the following relations:

$$x^j \equiv \sum_{m=0}^{\varphi(d)-1} c_{mj} x^m \bmod \Phi_d(x).$$

Define Z_j to be the j-th term in the sum of g_d. That is, for $0 \leq j \leq d-1$, we define

$$Z_j := \prod_{m=0}^{\varphi(d)-1} z_{m+1}^{c_{mj}}.$$

Thus we have $g_d(z_1, \ldots, z_{\varphi(d)}) = \sum_{j=1}^{d-1} Z_j$. Note that we have the following:

$$\prod_{j=1}^{d-1} Z_j = 1.$$

This is because taking the product of all Z_j corresponds to computing the sum

$$1 + x + x^2 + \cdots + x^{d-1},$$

which is equivalent to 0 modulo $\Phi_d(x)$ because $\Phi_d(x) \mid \frac{x^d-1}{x-1} = 1 + x + \cdots + x^{d-1}$. Thus the set $\{Z_0, \ldots, Z_{d-1}\}$ can be viewed as the eigenvalues of some special unitary matrix $U \in \mathrm{SU}(d)$.

Now, note that $U(1) = \mathbb{T}$ (the complex unit circle). Then, at the very least, we can define the following embeddings for any d:

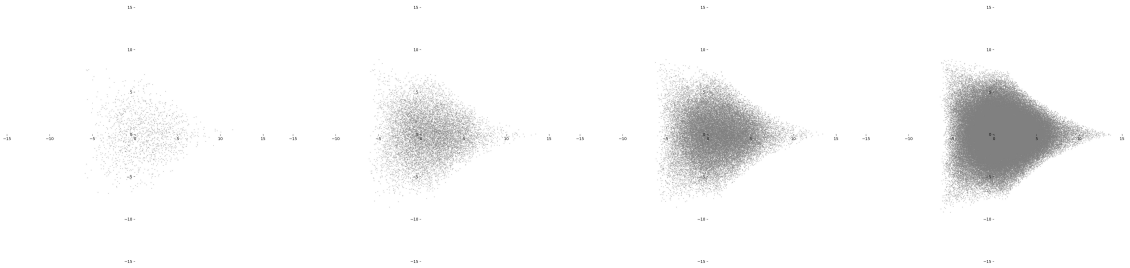
$$\xi_d : U(1)^{\varphi(d)} \hookrightarrow \mathrm{SU}(d), \qquad (z_1, \ldots, z_{\varphi(d)}) \mapsto \mathrm{diag}(Z_0, \ldots, Z_{d-1}),$$

where $\mathrm{diag}(Z_0, \ldots, Z_{d-1})$ is simply the matrix with the Z_j's in the diagonal entries and 0 everywhere else. Similar to the proof of the proposition, we again have that any element in $\mathrm{img}(g_d)$ can be realized as the trace of some matrix in $\mathrm{img}(\xi_d)$.

However, these embeddings don't provide us with any information we didn't already have. Thus we would like to extend these embeddings in some way that would prove helpful in describing the behavior of Gaussian periods and the animations of Gaussian periods. It is only because we can easily describe the case when d

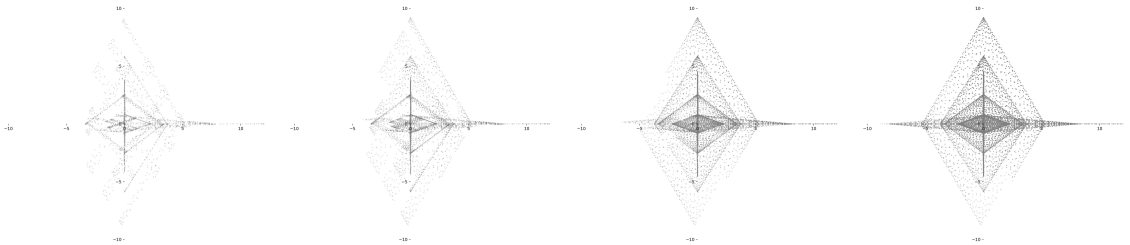
is prime that we are able to get the useful homomorphisms $\psi_d : U(1) \times \mathrm{SU}(d-1) \hookrightarrow \mathrm{SU}(d)$ in the proof of the proposition. As of the time of writing, this is still an area of active exploration.

Finally, we end this chapter by providing some still frames of Gaussian periods animations for situations outside of those described in Proposition 2.2. In Figure 2.2, we provide still frames for the case when $d = 15$ in the DGL Theorem, and in Figure 2.3, we provide still frames for a situation completely unrelated to the DGL Theorem.



(a) Up to $20\lfloor\sqrt[4]{n}\rfloor$ *(b)* Up to $150\lfloor\sqrt[4]{n}\rfloor$ *(c)* Up to $500\lfloor\sqrt[4]{n}\rfloor$ *(d)* Up to $2000\lfloor\sqrt[4]{n}\rfloor$

Figure 2.2. Still frames of Gaussian period animations for g_{15} when $n = 31^5$ and $\omega = 17404906$



(a) Up to $10\lfloor\sqrt{n}\rfloor$ *(b)* Up to $20\lfloor\sqrt{n}\rfloor$ *(c)* Up to $50\lfloor\sqrt{n}\rfloor$ *(d)* Up to $100\lfloor\sqrt{n}\rfloor$

Figure 2.3. Still frames of Gaussian period animations for a shape not related to the DGL Theorem when $n = 91205$ and $\omega = 1322$

CHAPTER 3

CHARACTER THEORY PERSPECTIVE

The work presented in this chapter includes and expands upon [Pla24, §3, 5], which is set to appear in the *International Journal of Number Theory*.

In this chapter, we explore Gaussian periods from the supercharacter theory perspective.

In particular, we start in Section 3.1 by defining a natural generalization of Gaussian periods, and we provide a proof to show that this natural generalization fits the definition of a supercharacter theory.

From there, the main goal of the rest of the chapter is to state, prove, and discuss Theorem 3.4, which is a broad generalization of the DGL Theorem using this newly defined supercharacter theory. The majority of Section 3.2 is dedicated to stating and proving this theorem, while Section 3.3 provides a discussion on the ways in which Theorem 3.4 cannot be generalized even further.

3.1 Analogue Using Supercharacter Theory

We now return to viewing Gaussian periods as values of a supercharacter theory. For the definition of a supercharacter theory, we refer the reader to Definition 1.5 in Section 1.5.

Recall that the supercharacter theory used in Gaussian periods is constructed using a cyclic subgroup $\langle\omega\rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$, where the supercharacters and superclasses are defined using a compatible action of $\langle\omega\rangle$ on the group $\mathbb{Z}/n\mathbb{Z}$ and its group of characters. We can generalize this setting in the following way.

Let $G = (\mathbb{Z}/n\mathbb{Z})^m$. The irreducible characters of G are simply products of irreducible characters on $\mathbb{Z}/n\mathbb{Z}$. That is, given $\mathbf{x} = (x_1, \ldots, x_m) \in G$, we obtain an

irreducible character $\chi_{\mathbf{x}} \in \hat{G}$ (the group of irreducible characters) such that for all $\mathbf{y} = (y_1, \ldots, y_m) \in G$, we have the following:

$$\chi_{\mathbf{x}}(\mathbf{y}) = \chi_{x_1}(y_1) \cdot \chi_{x_2}(y_2) \cdots \chi_{x_m}(y_m) = e\left(\frac{x_1 y_1 + \cdots + x_m y_m}{n}\right).$$

The analogy of $(\mathbb{Z}/n\mathbb{Z})^\times$ in this setting is the set of automorphisms $\mathrm{Aut}(G)$, which is isomorphic to $\mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$. Thus, we can choose a matrix $A \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ of order d, and take the cyclic subgroup $\Gamma := \langle A \rangle$. We then define the (right) action of Γ on G to be

$$\gamma \cdot \mathbf{x} = \gamma^T \mathbf{x},$$

where $\gamma \in \Gamma$, γ^T is the transpose of the matrix γ, and $\mathbf{x} \in G$ (viewed as a column vector). Let $\mathcal{K}$ be the partition of G corresponding to the orbits of this action. We also define the (right) action of Γ on $\hat{G}$ to be

$$\gamma \cdot \chi_{\mathbf{x}} = \chi_{\gamma^{-1}\mathbf{x}}$$

for $\chi_{\mathbf{x}} \in \hat{G}$. Let $\mathcal{X}$ be the partition of $\hat{G}$ corresponding to the orbits of this action. Then $(\mathcal{X}, \mathcal{K})$ defines a supercharacter theory on $(\mathbb{Z}/n\mathbb{Z})^m$.

This follows from a more general statement by Brumbaugh et al. at the beginning of Section 2 in [BBF+14]. While the authors of that paper did not state their result as a proposition, we do so here for the sake of clarity.

Proposition 3.1 (From Section 2 of [BBF+14])**.** *Let $G = (\mathbb{Z}/n\mathbb{Z})^m$, and let $\hat{G}$ be its group of characters. Let Γ be a subgroup of $GL_m(\mathbb{Z}/n\mathbb{Z})$, and let $\mathcal{K}$ and $\mathcal{X}$ be the partitions defined in the preceding paragraphs for G and $\hat{G}$, respectively. Then $(\mathcal{X}, \mathcal{K})$ is a supercharacter theory on G.*

Remark 3.2. In the paper of Brumbaugh et al., they require that Γ be a symmetric subgroup—i.e. that $\Gamma^T = \Gamma$. However, we note that this assumption is not used

until after the supercharacter theory axioms were proved, so it is not necessary for the statement of the proposition.

We also note that the group action defined in [BBF+14] differs slightly from the one we defined above. This slight difference does not alter the details of the proof. However, for the sake of clarity, we provide a proof of the proposition for the case when $\Gamma = \langle A \rangle$ and the action is defined as discussed above.

Proof. To check that $(\mathcal{X}, \mathcal{K})$ is a supercharacter theory on $(\mathbb{Z}/n\mathbb{Z})^m$, we first note that that $\{0\} \in \mathcal{K}$ by definition of our Γ-action on G.

To see that $|\mathcal{X}| = |\mathcal{K}|$, note that the orbits defining these partitions are simply cosets of Γ^{-1} and Γ^T, respectively. The cosets of both of these subgroups are in bijection with cosets of Γ, so the number of partitions in each set is the same.

We then need to show that for $X \in \mathcal{X}$, the supercharacter function

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

is constant on every $K \in \mathcal{K}$. First, note that an element $X \in \mathcal{X}$ is the Γ-orbit of some character $\chi_{\mathbf{x}} \in \hat{G}$. Thus $X = \{\chi_{\mathbf{x}}, \chi_{A^{-1}\mathbf{x}}, \ldots, \chi_{A^{-(d-1)}\mathbf{x}}\}$. Now let $K \in \mathcal{K}$, and note that if $\mathbf{k}$, $\mathbf{k}' \in K$, then there exists an exponent $j \in \{0, 1, \ldots, d-1\}$ such that $\mathbf{k} = (A^T)^j \mathbf{k}'$. We then have the following:

$$\begin{aligned}\sigma_X(\mathbf{k}) &= \chi_{\mathbf{x}}(\mathbf{k}) + \chi_{A^{-1}\mathbf{x}}(\mathbf{k}) + \cdots + \chi_{A^{-(d-1)}\mathbf{x}}(\mathbf{k}) \\ &= e\left(\frac{\mathbf{x}\cdot\mathbf{k}}{n}\right) + e\left(\frac{(A^{-1}\mathbf{x})\cdot\mathbf{k}}{n}\right) + \cdots + e\left(\frac{(A^{-(d-1)}\mathbf{x})\cdot\mathbf{k}}{n}\right).\end{aligned}$$

Let $i \in \{0, 1, \ldots, d-1\}$, and note that by the properties of the dot product, we have that

$$(A^i\mathbf{x})\cdot\mathbf{k}' = (A^i\mathbf{x})\cdot((A^T)^j\mathbf{k}) = (A^i\mathbf{x})\cdot((A^j)^T\mathbf{k}) = (A^jA^i\mathbf{x})\cdot\mathbf{k}.$$

(We note that it is this interaction with the dot product that caused us to define the action of Γ on G using the transpose.) We then have the following:

$$\begin{aligned}\sigma_X(\mathbf{k}') &= e\left(\frac{\mathbf{x}\cdot\mathbf{k}'}{n}\right) + e\left(\frac{(A^{-1}\mathbf{x})\cdot\mathbf{k}'}{n}\right) + \cdots + e\left(\frac{(A^{-(d-1)}\mathbf{x})\cdot\mathbf{k}'}{n}\right) \\ &= e\left(\frac{(A^{j}\mathbf{x})\cdot\mathbf{k}}{n}\right) + e\left(\frac{(A^{j-1}\mathbf{x})\cdot\mathbf{k}}{n}\right) + \cdots + e\left(\frac{(A^{j-(d-1)}\mathbf{x})\cdot\mathbf{k}}{n}\right) \\ &= e\left(\frac{\mathbf{x}\cdot\mathbf{k}}{n}\right) + e\left(\frac{(A^{-1}\mathbf{x})\cdot\mathbf{k}}{n}\right) + \cdots + e\left(\frac{(A^{-(d-1)}\mathbf{x})\cdot\mathbf{k}}{n}\right),\end{aligned}$$

where the final equality comes from reordering the summands and by using the fact that A has order d. Note that the sum in the final line is $\sigma_X(\mathbf{k})$, which shows that $\sigma_X(\mathbf{k}) = \sigma_X(\mathbf{k}')$. Since $\mathbf{k}, \mathbf{k}' \in K$ were arbitrary, then σ_X is constant on K as desired.

Thus $(\mathcal{X}, \mathcal{K})$ defines a supercharacter theory on $(\mathbb{Z}/n\mathbb{Z})^m$. □

Now, each irreducible character on G is given by a choice of vector $\mathbf{x} \in (\mathbb{Z}/n\mathbb{Z})^m$. In the case $m = 1$ (i.e. the case of Gaussian periods), we've seen that the matrix A is simply scalar multiplication. In order to get the vectors $\mathbf{x}$ used for the irreducible characters $\chi_{\mathbf{x}}$, we used the set of vectors given by the orbit $\langle A\rangle \cdot 1$, where 1 is the identity element in $(\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{GL}_1(\mathbb{Z}/n\mathbb{Z})$.

As noted in Proposition 2.2 of [DGL15], if we choose any nonzero $r \in \mathbb{Z}/n\mathbb{Z}$ and instead use the orbit $\langle A\rangle \cdot r$ to obtain our characters, then the corresponding plot of supercharacter values can be embedded within the plot corresponding to $r = 1$. In other words, the case when using $r = 1$ for the characters is the most general case possible, which then justifies our use of the orbit $\langle A\rangle \cdot 1$.

Analogously for the $m > 1$ case, the vectors used for the irreducible characters will be the set of vectors given by the orbit $\langle A\rangle \cdot \mathbf{1}$, where $\mathbf{1} = (1, 1, \ldots, 1)^T \in (\mathbb{Z}/n\mathbb{Z})^m$ is viewed as a column vector.

Finally, we are able to define the following generalization of Gaussian periods using the perspective of supercharacter theory.

Definition 3.3. For $\mathbf{x} \in (\mathbb{Z}/n\mathbb{Z})^m$, we define the following cyclic supercharacter:

$$\theta_{n,m,A} : (\mathbb{Z}/n\mathbb{Z})^m \to \mathbb{C}, \qquad \theta_{n,m,A}(\mathbf{x}) := \sum_{j=0}^{d-1} e\left(\frac{A^j \bullet \mathbf{x}}{n}\right),$$

where $A^j \bullet \mathbf{x}$ represents $(A^j\mathbf{1}) \cdot \mathbf{x}$; that is, the dot product between $A^j\mathbf{1}$ and $\mathbf{x}$. We call $\mathrm{img}(\theta_{n,m,A})$ the *cyclic supercharacter plot for n, m, and A*.

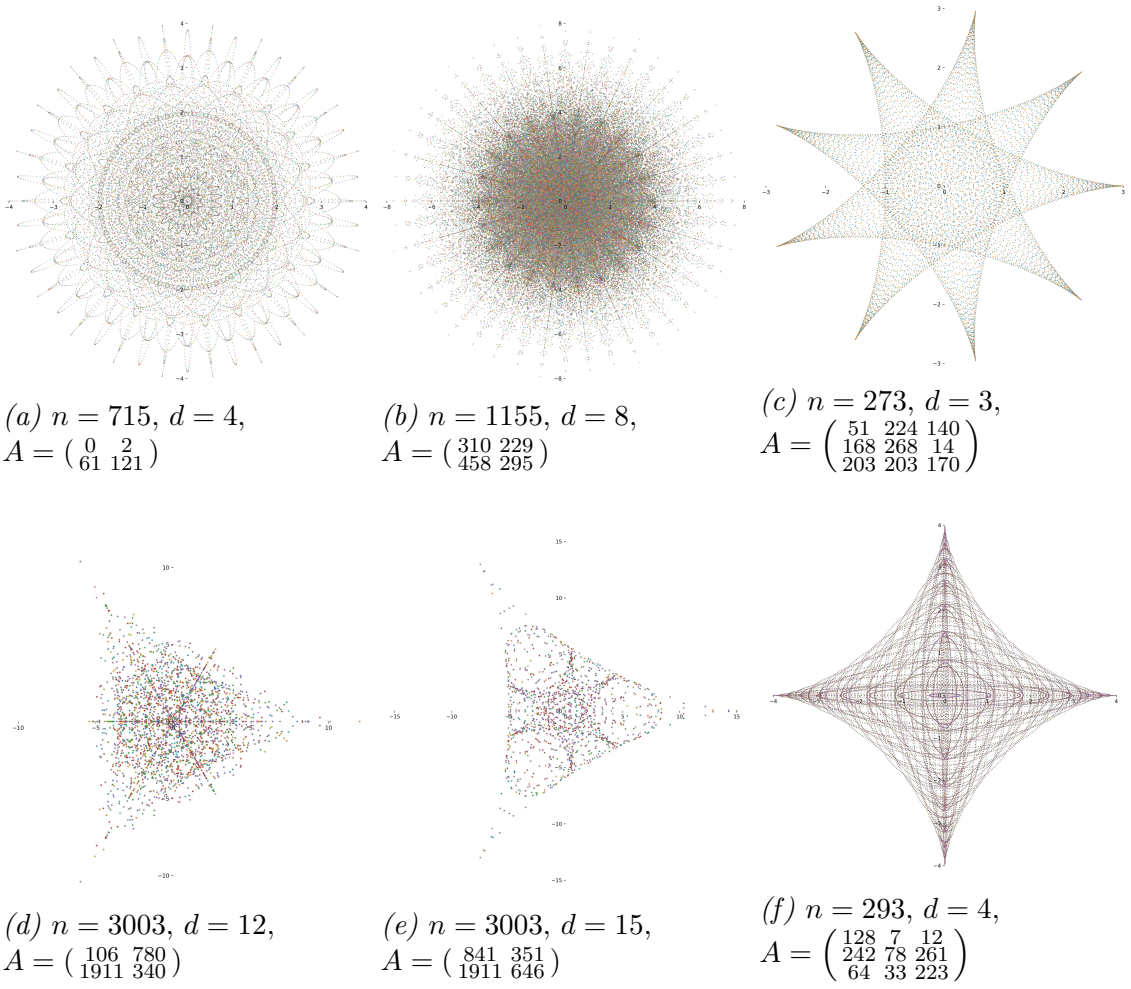
We provide examples of cyclic supercharacter plots in Figure 3.1.

It should be noted that we do not use any standardized coloring scheme for cyclic supercharacter plots. Recall from the end of Section 1.3 that the coloring scheme for Gaussian periods was determined by choosing a color modulus c. Two Gaussian periods $\eta_{n,\omega}(k)$ and $\eta_{n,\omega}(k')$ were then colored the same if $k \equiv k' \bmod c$. This sort of coloring scheme doesn't naturally extend to more general cyclic supercharacter plots in a useful way. Because of this, when generating these cyclic supercharacter plots, we simply let Python apply its automatic coloring to the points (it cycles through a list of colors).

3.2 Generalization of Duke–Garcia–Lutz Theorem

Now that we have generalized the definition of Gaussian periods to cyclic supercharacters on $(\mathbb{Z}/n\mathbb{Z})^m$, our goal is to prove the following generalization of the DGL Theorem.

Theorem 3.4 (Theorem 13 of [Pla24])**.** *Let $n \in \mathbb{Z}_{\geq 2}$ and $m \in \mathbb{Z}_{\geq 1}$. Suppose $d \mid (\#GL_m(\mathbb{Z}/n\mathbb{Z}))$, and let Φ_d be the d-th cyclotomic polynomial. Choose a matrix $A \in GL_m(\mathbb{Z}/n\mathbb{Z})$ such that the order of A is d and $\Phi_d(A) = 0$ in $Mat_m(\mathbb{Z}/n\mathbb{Z})$. Let*



(a) $n = 715$, $d = 4$, $A = \begin{pmatrix} 0 & 2 \\ 61 & 121 \end{pmatrix}$

(b) $n = 1155$, $d = 8$, $A = \begin{pmatrix} 310 & 229 \\ 458 & 295 \end{pmatrix}$

(c) $n = 273$, $d = 3$, $A = \begin{pmatrix} 51 & 224 & 140 \\ 168 & 268 & 14 \\ 203 & 203 & 170 \end{pmatrix}$

(d) $n = 3003$, $d = 12$, $A = \begin{pmatrix} 106 & 780 \\ 1911 & 340 \end{pmatrix}$

(e) $n = 3003$, $d = 15$, $A = \begin{pmatrix} 841 & 351 \\ 1911 & 646 \end{pmatrix}$

(f) $n = 293$, $d = 4$, $A = \begin{pmatrix} 128 & 7 & 12 \\ 242 & 78 & 261 \\ 64 & 33 & 223 \end{pmatrix}$

Figure 3.1. Examples of cyclic supercharacter plots for various n, m, and A.

$\theta_{n,m,A} : (\mathbb{Z}/n\mathbb{Z})^m \to \mathbb{C}$ be the cyclic supercharacter corresponding to n, m, and A. Then $img(\theta_{n,m,A})$ is contained in the image of the Laurent polynomial $g_d : \mathbb{T}^{\varphi(d)} \to \mathbb{C}$ defined by the following:

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

where the c_{jk} are given by the relations

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

Additionally, for a fixed d, and as n tends to infinity—assuming there exists a matrix $A \in GL_m(\mathbb{Z}/n\mathbb{Z})$ such that $\Phi_d(A) = 0 \bmod n$—every nonempty open disk in $img(g_d)$ eventually contains points in $img(\theta_{n,m,A})$. In other words, the image of g_d is "filled out" by cyclic supercharacter plots as the modulus grows without bound.

Before we begin the proof of Theorem 3.4, we make some necessary detours. First, some remarks about the statement of this theorem, starting with a discussion of the areas in which this generalizes the DGL Theorem.

Remark 3.5. There are two directions in which this theorem generalizes the original DGL Theorem. First, it concerns the group $(\mathbb{Z}/n\mathbb{Z})^m$ for any $m \geq 1$, rather than just the case $m = 1$. Second, it allows for composite moduli n, with the restriction that there is some matrix $A \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ which both has order d and satisfies $\Phi_d(A) = 0 \bmod n$. To see why this new condition on n truly is a generalization, recall that the DGL Theorem assumes the modulus is p^e for some power of an odd prime p. The group being studied is $\mathbb{Z}/p^e\mathbb{Z}$, and the group of automorphisms is

$$\mathrm{GL}_1(\mathbb{Z}/p^e\mathbb{Z}) \cong (\mathbb{Z}/p^e\mathbb{Z})^\times.$$

Since $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is cyclic when p is odd, then if $d \mid \#(\mathbb{Z}/p^e\mathbb{Z})^\times$, there is always an element $\omega \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ of order d (in general, note that there is not always a matrix $A \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ of order d whenever $d \mid \#\mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$). Additionally, in the case where $m = 1$, the order d divides $p-1$ if and only if $\Phi_d(\omega) = 0 \bmod p^e$. That is, if ω has order $d \mid (p-1)$, then it automatically satisfies the equation $\Phi_d(\omega) = 0 \bmod p^e$. However, when $m > 1$ or n is not a power of an odd prime, this condition is not automatically satisfied when $A \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ has order d. With this in mind, Theorem 3.4 generalizes the DGL Theorem using matrices which satisfy Φ_d rather than simply using matrices which have order d (without necessarily satisfying Φ_d).

Remark 3.6. Note that Remark 3.5 hints at the possibility of another generalization of the DGL Theorem. The fact that $A \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ has order d implies that the minimal polynomial of A must divide $x^d - 1$. When we additionally assume that $m = 1$ and n is a power of an odd prime, then the minimal polynomial is always $\Phi_d(x)$. However, this is not guaranteed when $m > 1$ or when n isn't a power of an odd prime, so one might then wonder if anything can be said about the behavior of $\theta_{n,m,A}$ when $\Phi_d(A) \neq 0 \bmod n$. It turns out that while we can still describe the general shape of $\mathrm{img}(\theta_{n,m,A})$, we are no longer guaranteed the asymptotic filling out behavior. We discuss this issue in more detail in Section 3.3.

An astute reader might have the following question after reading Theorem 3.4: How do we know that there are infinitely many n such that $\mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ contains a matrix A of order d such that $\Phi_d(A) = 0 \bmod n$? This is a natural question, as the statement on the asymptotic behavior of $\theta_{n,m,A}$ doesn't make sense without the existence of such n. In the following remark, we provide a simple construction that shows there are infinitely many n with the stated properties.

Remark 3.7. Let m and d be given. Since there are infinitely many primes congruent to 1 mod d, then we can choose an infinite sequence of odd primes $p_1 < p_2 < p_3 < \ldots$ such that $p_i = 1 \bmod d$ for every i. For each i, choose $\omega_i \in (\mathbb{Z}/p_i\mathbb{Z})^\times$ such that the order of ω_i is d; such an ω_i exists because $(\mathbb{Z}/p_i\mathbb{Z})^\times$ is cyclic of order $p_i - 1$, which is divisible by d. We can then choose the matrix $A_i \in \mathrm{GL}_m(\mathbb{Z}/p_i\mathbb{Z})$ to be the matrix $\mathrm{diag}(\omega_i, \omega_i, \ldots, \omega_i)$. That is, A_i comes from the diagonal embedding

$$((\mathbb{Z}/p_i\mathbb{Z})^\times)^m \hookrightarrow \mathrm{GL}_m(\mathbb{Z}/p_i\mathbb{Z}), \qquad \alpha \mapsto \mathrm{diag}(\alpha, \alpha, \ldots, \alpha).$$

Since $\Phi_d(\omega_i) = 0 \bmod p_i$ for every i (as mentioned in Remark 3.5), then $\Phi_d(A_i) = 0 \bmod p_i$ for every i.

There are, of course, more interesting examples of moduli n and matrices A such that $\Phi_d(A) = 0 \bmod n$. The example above is used simply to show the existence of infinitely many n with the desired properties.

We now work toward the proof of Theorem 3.4, which has two main parts. First, we must show that $\mathrm{img}(\theta_{n,m,A})$ is contained in $\mathrm{img}(g_d)$, which will come directly from the fact that $\Phi_d(A) = 0 \bmod n$. And second, we must show that the $\mathrm{img}(g_d)$ is filled out asymptotically as described. In order to describe the asymptotic behavior of these cyclic supercharacters, we need the following concepts about equidistribution. We note that these concepts are those used by Katz in [Kat12], though we borrow the notational conventions used by Kowalski in [Kow13].

Definition 3.8. Let Y a nonempty finite set. Let s be a positive integer, and suppose we have a map

$$\Lambda : Y \to [0,1)^s, \qquad \mathbf{y} \mapsto \Lambda(\mathbf{y}) := (\Lambda_1(y_1), \Lambda_2(y_2), \ldots, \Lambda_s(y_s)).$$

The *discrepancy* of (Y, Λ) is defined to be

$$\sup_B \left| \frac{\#\{\mathbf{y} \in Y : \Lambda(\mathbf{y}) \in B\}}{\#Y} - \mathrm{vol}(B) \right|,$$

where the supremum is taken over all boxes $B = [a_1, b_1) \times \cdots \times [a_s, b_s) \subseteq [0,1)^s$ and $\mathrm{vol}(B)$ denotes the volume of B. We say that a sequence $(Y_t, \Lambda_t)_{t=1}^{\infty}$ of nonempty finite sets Y_t and maps $\Lambda_t : Y_t \to [0,1)^s$ is *uniformly distributed mod 1* if the discrepancy of Λ_t goes to zero as $t \to \infty$.

Remark 3.9. We should note here that this definition differs from the definition given in [DGL15, GHL15] (and several other places in the literature). In particular, the discrepancy in those papers is defined using the proportion

$$\frac{\#(\Lambda(Y) \cap B)}{\#\Lambda(Y)}$$

rather than the proportion

$$\frac{\#\{\mathbf{y} \in Y : \Lambda(\mathbf{y}) \in B\}}{\#Y}.$$

That is, they determine the proportion of distinct elements of the image which are in B. The correct definition of discrepancy, however, is interested in the number of *indices* $\mathbf{y}$ whose image is in B. These two definitions are not equivalent, as Λ is not necessarily injective.[1]

Remark 3.10. If $(Y_t, \Lambda_t)_{t=1}^{\infty}$ is a sequence which is uniformly distributed mod 1, then it is an easy consequence that $\Lambda_t(Y_t)$ become dense in $[0,1)^s$. In fact, it implies the stronger statement that $\Lambda_t(Y_t)$ becomes *equidistributed* in $[0,1)^s$—i.e. that its points become "evenly spaced." While we care primarily about the density result for the purposes of proving Theorem 3.4, the result on equidistribution is interesting in its own right, and we discuss this briefly in Remark 3.12 after the proof.

We now offer Weyl's criterion (stated as Lemma 1 in [GHL15]) for determining if a sequence is uniformly distributed mod 1. This will be a critical lemma in our proof of Theorem 3.4.

Lemma 3.11 (Weyl's Criterion)**.** *A sequence $(Y_t, \Lambda_t)_{t=1}^{\infty}$ of nonempty finite sets Y_t and maps $\Lambda_t : Y_t \to [0,1)^s$ is uniformly distributed mod 1 if and only if for every nonzero $\mathbf{v} \in \mathbb{Z}^s$, we have*

$$\lim_{t\to\infty} \frac{1}{\#Y_t} \sum_{\mathbf{y}\in Y_t} e(\Lambda_t(\mathbf{y}) \cdot \mathbf{v}) = 0,$$

where $\Lambda_t(\mathbf{y}) \cdot \mathbf{v}$ denotes the usual dot product.

We are now ready to prove Theorem 3.4.

[1]This error in definition was pointed out by an anonymous referee for a paper that this author submitted on these topics. The author would like to thank the referee for this correction.

Proof. First, we show that $\text{img}(\theta_{n,m,A}) \subseteq \text{img}(g_d)$. Let n, d, and A have the properties as stated in the theorem. Since we assume that $\Phi_d(A) = 0 \bmod n$, then for $k \in \{0, 1, \ldots, d-1\}$, we obtain the relations

$$A^k \equiv \sum_{j=0}^{\varphi(d)-1} c_{jk} A^j \bmod n,$$

where the c_{jk} are the constants mentioned in the statement of the theorem. Then for any $\mathbf{x} \in (\mathbb{Z}/n\mathbb{Z})^m$, we now have the following:

$$\theta_{n,m,A}(\mathbf{x}) = \sum_{k=0}^{d-1} e\left(\frac{A^k \bullet \mathbf{x}}{n}\right) = \sum_{k=0}^{d-1} e\left(\frac{\sum_{j=0}^{\varphi(d)-1} c_{jk} A^j \bullet \mathbf{x}}{n}\right) = \sum_{k=0}^{d-1} \prod_{j=0}^{\varphi(d)-1} e\left(\frac{A^j \bullet \mathbf{x}}{n}\right)^{c_{jk}}.$$

Since $e\left(\dfrac{A^j \bullet \mathbf{x}}{n}\right)$ is contained in $\mathbb{T}$ for all j, then the fact that $\text{img}(\theta_{n,m,A}) \subseteq \text{img}(g_d)$ follows from the definition of g_d.

We now need to show that $\text{img}(\theta_{n,m,A})$ fills out $\text{img}(g_d)$ as $n \to \infty$. To do this, we need to prove that the roots of unity showing up in the supercharacter sums get asymptotically close to any element $(z_1, \ldots, z_{\varphi(d)})$ in the domain of g_d. We show this by proving that the exponents of those roots of unity are uniformly distributed mod 1, which we do by using Weyl's criterion.

We start by indexing our sets Y_n and maps Λ_n in the following way. Let $\mathcal{N} \subseteq \mathbb{N}$ be the set of all positive integers n such that $\text{GL}_m(\mathbb{Z}/n\mathbb{Z})$ contains a matrix A of order d such that $\Phi_d(A) = 0 \bmod n$. Create a sequence $(n_i)_{i=1}^{\infty}$ using the elements of $\mathcal{N}$, indexed so that $n_1 < n_2 < n_3 < \cdots$. Additionally, let A_i denote our choice of matrix of order d modulo n_i. We let $Y_{n_i} := (\mathbb{Z}/n_i\mathbb{Z})^m$. Then we define the maps $\Lambda_{n_i} : Y_{n_i} \to [0,1)^{\varphi(d)}$ by the following:

$$\Lambda_{n_i}(\mathbf{y}) = \left(\frac{(A_i^0 \bullet \mathbf{y}) \bmod n_i}{n_i}, \frac{(A_i^1 \bullet \mathbf{y}) \bmod n_i}{n_i}, \ldots, \frac{(A_i^{\varphi(d)-1} \bullet \mathbf{y}) \bmod n_i}{n_i}\right).$$

Our goal, then, is to show that $(Y_{n_i}, \Lambda_{n_i})_{i=1}^{\infty}$ is uniformly distributed mod 1. Thus, using Lemma 3.11, we need to show that for any nonzero vector $\mathbf{v} \in \mathbb{Z}^{\varphi(d)}$,

the following is true:

$$\lim_{i\to\infty} \frac{1}{\#Y_{n_i}} \sum_{\mathbf{y}\in Y_{n_i}} e(\Lambda_{n_i}(\mathbf{y})\cdot\mathbf{v}) = 0.$$

Note that $\#Y_{n_i} = n_i^m$ for every i, so we need to show that

$$\lim_{i\to\infty} \frac{1}{n_i^m} \sum_{\mathbf{y}\in Y_{n_i}} e(\Lambda_{n_i}(\mathbf{y})\cdot\mathbf{v}) = 0.$$

To this end, first let us consider the vectors $A_i^j\mathbf{1}$ more closely. For

$$j \in \{0, 1, \ldots, \varphi(d)-1\},$$

we write $A_i^j =: (a_{bc,i}^j)_{1\le b,c\le m}$. Then we have the following:

$$A_i^j\mathbf{1} = A_i^j \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}^T = \begin{pmatrix} \sum_{c=1}^m a_{1c,i}^j & \sum_{c=1}^m a_{2c,i}^j & \cdots & \sum_{c=1}^m a_{mc,i}^j \end{pmatrix}^T.$$

Let us write $A_i^j\mathbf{1} = (w_{1,i}^j, w_{2,i}^j, \ldots, w_{m,i}^j)^T$. That is, the vector component $w_{k,i}^j$ is the sum of the elements in the k-th row of the matrix A_i^j. To simplify notation, we set $\mathbf{w}_i^j := A_i^j\mathbf{1} = (w_{1,i}^j, w_{2,i}^j, \ldots, w_{m,i}^j)^T$.

Returning to the computation at hand, let $\mathbf{v} = (v_0, \ldots, v_{\varphi(d)-1})$ be any nonzero vector in $\mathbb{Z}^{\varphi(d)}$. Then we have the following:

$$\begin{aligned}
\sum_{\mathbf{y}\in Y_{n_i}} e(\Lambda_{n_i}(\mathbf{y})\cdot\mathbf{v}) &= \sum_{\mathbf{x}\in(\mathbb{Z}/n_i\mathbb{Z})^m} e\left(\sum_{j=0}^{\varphi(d)-1} \frac{\mathbf{w}_i^j\cdot\mathbf{x}\cdot v_j}{n_i}\right) \\
&= \sum_{x_1,\ldots,x_m=0}^{n_i-1} e\left(\sum_{j=0}^{\varphi(d)-1} \frac{(w_{1,i}^j x_1 + w_{2,i}^j x_2 + \cdots + w_{m,i}^j x_m)v_j}{n_i}\right) \\
&= \left[\sum_{x_1=0}^{n_i-1} e\left(\sum_{j=0}^{\varphi(d)-1} \frac{w_{1,i}^j x_1 v_j}{n_i}\right)\right] \cdots \left[\sum_{x_m=0}^{n_i-1} e\left(\sum_{j=0}^{\varphi(d)-1} \frac{w_{m,i}^j x_m v_j}{n_i}\right)\right].
\end{aligned}$$

For $\ell \in \{1, \ldots, m\}$, we define $\alpha_{\ell,i} := \sum_{j=0}^{\varphi(d)-1} w_{\ell,i}^j \cdot v_j$. Then we have the following:

$$\sum_{\mathbf{y}\in Y_{n_i}} e(\Lambda_{n_i}(\mathbf{y})\cdot\mathbf{v}) = \left[\sum_{x_1=0}^{n_i-1} e\left(\sum_{j=0}^{\varphi(d)-1} \frac{w_{1,i}^j x_1 v_j}{n_i}\right)\right] \cdots \left[\sum_{x_m=0}^{n_i-1} e\left(\sum_{j=0}^{\varphi(d)-1} \frac{w_{m,i}^j x_m v_j}{n_i}\right)\right]$$

$$= \left[\sum_{x_1=0}^{n_i-1} e\left(\frac{\alpha_{1,i}x_1}{n_i}\right)\right] \cdots \left[\sum_{x_m=0}^{n_i-1} e\left(\frac{\alpha_{m,i}x_m}{n_i}\right)\right]$$

$$= \begin{cases} n_i^m & \text{if } n_i \mid \alpha_{\ell,i} \text{ for all } \ell \in \{1, 2, \ldots, m\}, \\ 0 & \text{otherwise.} \end{cases}$$

The final equality comes from the orthogonality of additive characters on $\mathbb{Z}/n\mathbb{Z}$. That is,

$$\sum_{x=0}^{n-1} e\left(\frac{\alpha x}{n}\right) = \begin{cases} n & \text{if } n \mid \alpha, \\ 0 & \text{otherwise.} \end{cases}$$

From here, we will show that there are at most finitely many i such that n_i divides $\alpha_{\ell,i}$ for all $\ell \in \{1, 2, \ldots, m\}$. First, define a polynomial

$$f_{\mathbf{v}}(x) = v_0 + v_1 x + \cdots + v_{\varphi(d)-1} x^{\varphi(d)-1} \in \mathbb{Z}[x].$$

Using the definition of $\alpha_{\ell,i}$, it is a simple calculation to check that the following equality holds:

$$f_{\mathbf{v}}(A_i) \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}^T = \begin{pmatrix} \alpha_{1,i} & \alpha_{2,i} & \cdots & \alpha_{m,i} \end{pmatrix}^T.$$

Consider now the cyclotomic polynomial $\Phi_d(x)$, which is irreducible over $\mathbb{Q}$ of degree $\varphi(d)$. Since $f_{\mathbf{v}}(x)$ has degree $\varphi(d) - 1$, then $\gcd(f_{\mathbf{v}}(x), \Phi_d(x)) = 1$ in $\mathbb{Q}[x]$. Thus there exist polynomials $P(x), Q(x) \in \mathbb{Q}[x]$ such that

$$P(x) f_{\mathbf{v}}(x) + Q(x)\Phi_d(x) = 1.$$

By clearing out denominators, we then obtain polynomials $R(x), S(x) \in \mathbb{Z}[x]$ such that

$$R(x) f_{\mathbf{v}}(x) + S(x)\Phi_d(x) = t$$

for some fixed nonzero integer t.

Note that the above equality depends only on the choice of d and the vector $\mathbf{v} \in \mathbb{Z}^{\varphi(d)}$, which we fixed at the beginning of the proof. In particular, the equality does not depend on the choices of n_i nor A_i. Thus for any of our chosen A_i, we find that

$$R(A_i)f_{\mathbf{v}}(A_i) + S(A_i)\Phi_d(A_i) = t \cdot I_m,$$

where I_m is the $m \times m$ identity matrix. Since $\Phi_d(A_i) = 0 \bmod n_i$, we then find that

$$R(A_i)f_{\mathbf{v}}(A_i) \equiv t \cdot I_m \bmod n_i.$$

After multiplying both sides of this congruence by the matrix $\begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}^T$, we get the following result:

$$R(A_i)f_{\mathbf{v}}(A_i)\begin{pmatrix} 1 & \cdots & 1 \end{pmatrix}^T \equiv \begin{pmatrix} t & \cdots & t \end{pmatrix}^T \bmod n_i.$$

Now, $R(A_i)$ is an $m \times m$ matrix, so write $R(A_i) = (\rho_{bc,i})_{1 \le b,c \le m}$. Using the fact that

$$f_{\mathbf{v}}(A_i)\begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}^T = \begin{pmatrix} \alpha_{1,i} & \alpha_{2,i} & \cdots & \alpha_{m,i} \end{pmatrix}^T,$$

we can rewrite $R(A_i)f_{\mathbf{v}}(A_i)\begin{pmatrix} 1 & \cdots & 1 \end{pmatrix}^T$ as the following:

$$\begin{pmatrix} \rho_{11,i} & \cdots & \rho_{1m,i} \\ \vdots & \ddots & \vdots \\ \rho_{m1,i} & \cdots & \rho_{mm,i} \end{pmatrix}\begin{pmatrix} \alpha_{1,i} & \cdots & \alpha_{m,i} \end{pmatrix}^T = \begin{pmatrix} \sum_{\ell=1}^{m} \rho_{1\ell,i}\alpha_{\ell,i} & \sum_{\ell=1}^{m} \rho_{2\ell,i}\alpha_{\ell,i} & \cdots & \sum_{\ell=1}^{m} \rho_{m\ell,i}\alpha_{\ell,i} \end{pmatrix}^T.$$

Putting this all together, we end up with the following equivalence relation:

$$\begin{pmatrix} \sum_{\ell=1}^{m} \rho_{1\ell,i}\alpha_{\ell,i} & \sum_{\ell=1}^{m} \rho_{2\ell,i}\alpha_{\ell,i} & \cdots & \sum_{\ell=1}^{m} \rho_{m\ell,i}\alpha_{\ell,i} \end{pmatrix}^T \equiv \begin{pmatrix} t & \cdots & t \end{pmatrix}^T \bmod n_i.$$

If we now assume that n_i divides $\alpha_{\ell,i}$ for every ℓ, then

$$\sum_{\ell=1}^{m} \rho_{b\ell,i}\alpha_{\ell,i}$$

is divisible by n_i for every $b \in \{1, \ldots, m\}$. Since

$$\sum_{\ell=1}^{m} \rho_{b\ell,i}\alpha_{\ell,i} \equiv t \bmod n_i$$

by the equivalence relation above, then n_i must also divide t. However, as stated previously, t is a nonzero integer which is fixed for all choices of n_i and A_i. Since there are at most finitely many i such that n_i divides t, then there can be at most finitely many i such that n_i divides $\alpha_{\ell,i}$ for all ℓ.

We can then choose N to be the largest integer such that n_N divides $\alpha_{\ell,N}$ for all ℓ, letting $N = 0$ if there is no such integer. Then for every $i > N$, the previous paragraph implies that

$$\sum_{\mathbf{y} \in Y_{n_i}} e(\Lambda_{n_i}(\mathbf{y}) \cdot \mathbf{v}) = 0.$$

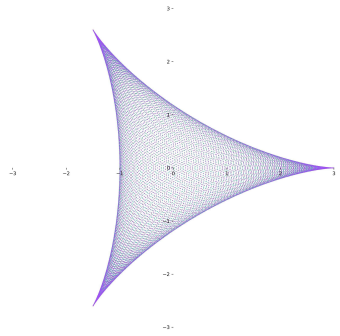
Hence, we have shown that

$$\lim_{i \to \infty} \frac{1}{\#Y_{n_i}} \sum_{\mathbf{y} \in Y_{n_i}} e(\Lambda_{n_i}(\mathbf{y}) \cdot \mathbf{v}) = 0.$$

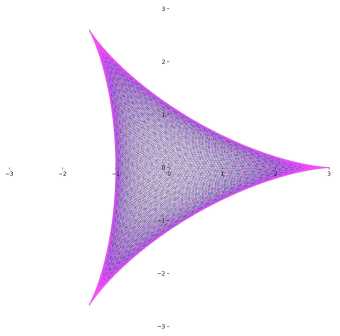
Thus the sequence $(Y_{n_i}, \Lambda_{n_i})_{i=1}^{\infty}$ is uniformly distributed mod 1 by Weyl's criterion, finishing our proof of Theorem 3.4. □

Remark 3.12. As mentioned in Remark 3.10, we showed not only that $\Lambda_{n_i}(Y_{n_i})$ becomes dense in $[0,1)^{\varphi(d)}$, but that it becomes equidistributed as well. More precisely, Theorem 3.4 shows that the sequence $(Y_{n_i}, \theta_{n_i,m,A_i})_{i=1}^{\infty}$ becomes equidistributed in $\mathrm{img}(g_d)$ with respect to the pushforward measure $(g_d)_*\lambda$ of the Haar measure λ on $\mathbb{T}^{\varphi(d)}$. These concepts and more are explored in much more depth in the aforementioned papers by Untrau and Kowalski–Untrau [Unt24, KU23].

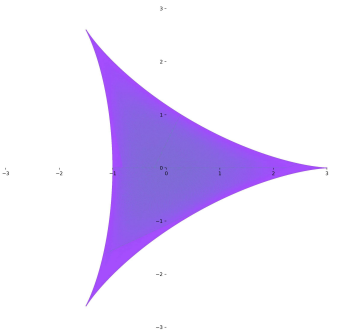
To conclude this section, we include some examples of the phenomenon described in Theorem 3.4 in Figure 3.2.



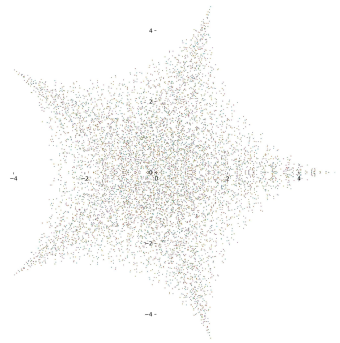
(a) $n = 7 \cdot 13 \cdot 19$, $d = 3$, $A = 2629$



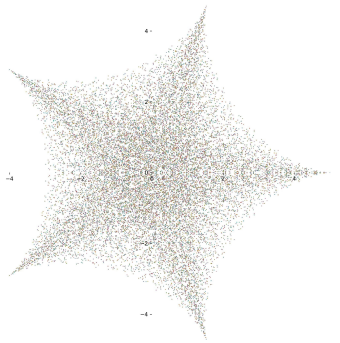
(b) $n = 7^2 13^2 19$, $d = 3$, $A = 21823$



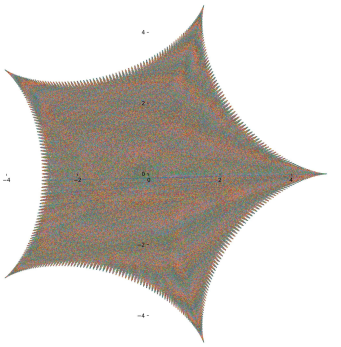
(c) $n = 7^2 13^2 19 \cdot 31$, $d = 3$, $A = 109827$



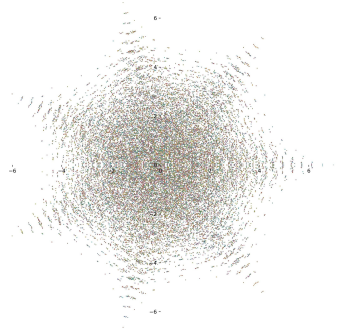
(d) $n = 11 \cdot 19$, $d = 5$, $A = \left(\begin{smallmatrix} 0 & 1 \\ 94 & 166 \end{smallmatrix}\right)$



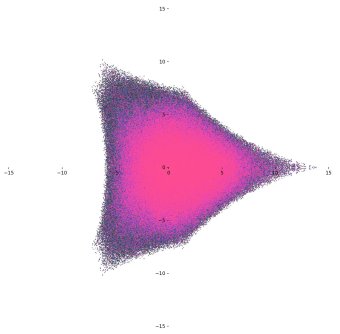
(e) $n = 11 \cdot 29$, $d = 5$, $A = \left(\begin{smallmatrix} 0 & 1 \\ 173 & 266 \end{smallmatrix}\right)$



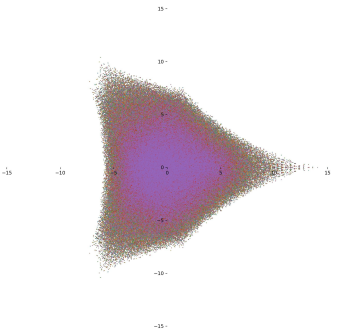
(f) $n = 11^2 29$, $d = 5$, $A = \left(\begin{smallmatrix} 0 & 3508 \\ 1 & 2383 \end{smallmatrix}\right)$



(g) $n = 2 \cdot 43$, $d = 7$, $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 19 \\ 0 & 1 & 18 \end{pmatrix}$



(h) $n = 31 \cdot 61^2 181$, $d = 15$, $A = 49676$



(i) $n = 83$, $d = 15$, $A = \begin{pmatrix} 0 & 0 & 0 & 82 \\ 1 & 0 & 0 & 52 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 32 \end{pmatrix}$

Figure 3.2. Examples of Theorem 3.4

3.3 Barriers to Further Generalized Results

We now return to our discussion in Remark 3.6. Let n, m, and d be chosen as in Theorem 3.4. Let $A \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ have order d, but this time assume that $\Phi_d(A) \neq 0 \bmod n$. In this section, we discuss the implications of these assumptions, and we show by counterexample that (an appropriate generalization of) Theorem 3.4 does not hold.

First, note that $A^d - I = 0 \bmod n$ since A has order d in $\mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$. Also, recall that $x^d - 1 \in \mathbb{Z}[x]$ decomposes as

$$x^d - 1 = \prod_{k|d} \Phi_k(x).$$

Thus the divisors of $x^d - 1$ are of the form $\Phi_{k_1}\Phi_{k_2}\cdots\Phi_{k_\ell}$ for k_i dividing d. Let $R \subseteq \mathbb{Z}[x]$ be the set of polynomials $f(x)$ dividing $x^d - 1$ such that $f(A) = 0 \bmod n$. At the very least, we know that $x^d - 1 \in R$, though it may not be the polynomial in R with the smallest degree.

Let $\mu(x) \in R$ be the monic polynomial with minimal degree among the polynomials in R. If $\mu(x)$ is irreducible over $\mathbb{Z}$, then $\mu = \Phi_d$ (since A has order d). However, since we are exploring the case where $\Phi_d(A) \neq 0 \bmod n$, then we assume that μ is reducible over $\mathbb{Z}$.

It turns out that Theorem 3.4 does not generalize to situations where μ is reducible. At least, the asymptotic filling out behavior no longer holds—however, we can still describe the general shape of the supercharacter values. For example, given $\mu(x) \mid (x^d - 1)$, we can define an analogous Laurent polynomial $g_\mu : \mathbb{T}^{\deg(\mu)} \to \mathbb{C}$ given by the following:

$$g_\mu(z_1, \ldots, z_{\deg(\mu)}) = \sum_{k=0}^{d-1} \prod_{j=0}^{\deg(\mu)-1} z_{j+1}^{b_{jk}},$$

where the b_{jk} are given by the relations

$$x^k \equiv \sum_{j=0}^{\deg(\mu)-1} b_{jk} x^j \bmod \mu(x).$$

Then, using the same reasoning as in the proof of Theorem 3.4, we see that

$$\mathrm{img}(\theta_{n,m,A}) \subseteq \mathrm{img}(g_\mu).$$

However, it is no longer necessarily true that $\mathrm{img}(g_\mu)$ is filled out as $n \to \infty$. In fact, we provide a counterexample to this in the following paragraphs.

Recall that Weyl's criterion gives an equivalent condition for $\mathrm{img}(g_\mu)$ to be filled out asymptotically. This criterion says that $\mathrm{img}(g_\mu)$ is filled out asymptotically if for any nonzero $\mathbf{v} \in \mathbb{Z}^{\deg(\mu)}$, we have

$$\lim_{i\to\infty} \frac{1}{\#Y_{n_i}} \sum_{\mathbf{y}\in Y_{n_i}} e(\Lambda_{n_i}(\mathbf{y}) \cdot \mathbf{v}) = 0,$$

where the Y_{n_i} and Λ_{n_i} are defined analogously to the proof of Theorem 3.4. Additionally, we showed in our proof that Weyl's criterion holds in the setting of Theorem 3.4 if and only if $f_{\mathbf{v}}(A_i)\mathbf{1} = 0 \bmod n_i$ for at most finitely many i. Thus finding a counterexample is equivalent to finding n_i, m, d, and A_i such that for some nonzero $\mathbf{v} \in \mathbb{Z}^{\deg(\mu)}$, we have $f_{\mathbf{v}}(A_i)\mathbf{1} = 0 \bmod n_i$ for infinitely many i.

To this end, consider the case where $\mu(x) = \Phi_3(x)\Phi_5(x)$; where $m = 6$ and $d = 15$; where n_i are the integers greater than 6 which are not divisible by 2, 3, or 5; and where A_i is fixed for all i to be the companion matrix to $\Phi_3\Phi_5$. Since $m = 6$ and $n_i \geq 7$, then it is guaranteed that $15 \mid (\#\mathrm{GL}_m(\mathbb{Z}/n_i\mathbb{Z}))$; to see this, consult the first bullet point in Section 3.4 and note that $3 \mid (p^2 - 1)$ and $5 \mid (p^4 - 1)$ for all primes $p \geq 7$. Additionally, if $A \in \mathrm{GL}_6(\mathbb{Z})$ is the companion matrix to $\Phi_3\Phi_5$, then A has order 15 (by properties of cyclotomic polynomials and companion matrices). One can then verify computationally that for all $k \in \{0, 1, \ldots, 14\}$, the

matrices A^k have integer entries in the set $\{0, \pm 1, \pm 2, \pm 3, \pm 4\}$. Thus, as long as n_i is not divisible by 2, 3, or 5, the matrix A has order 15 in the group $\mathrm{GL}_6(\mathbb{Z}/n_i\mathbb{Z})$. In particular, this means that no smaller power of A reduces to the identity modulo n_i.

We then choose the vector $\mathbf{v} = (1, 1, 1, 1, 1, 0) \in \mathbb{Z}^{\deg(\mu)}$ so that

$$f_{\mathbf{v}}(x) = 1 + x + x^2 + x^3 + x^4 = \Phi_5(x).$$

One can compute directly that

$$f_{\mathbf{v}}(A)\mathbf{1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^T,$$

where the multiplication is happening over $\mathbb{Z}$. Since $f_{\mathbf{v}}(A)\mathbf{1} = 0$ over $\mathbb{Z}$, then $f_{\mathbf{v}}(A)\mathbf{1} = 0 \bmod n_i$ for all n_i. Thus $\mathrm{img}(g_\mu)$ does *not* get filled out asymptotically.

Thus, without any added assumptions, Theorem 3.4 seems to be the most general version possible of the original DGL Theorem.

3.4 Computational Strategies and Heuristics

We end this chapter by discussing some of the computational strategies and heuristics that are useful for anyone interested in experimenting with Gaussian periods and cyclic supercharacters.

First, from a computational perspective, time complexity is the main constraint that restricts which examples can be generated. An astute reader might have already noticed that our choices for moduli in our examples are often fairly small, especially outside of a few examples of Gaussian period plots where some moduli were seven or eight digits long. This is, of course, almost entirely due to the quickly increasing number of computations needed as the modulus grows larger. For example, generating cyclic supercharacter plots for $G = (\mathbb{Z}/n\mathbb{Z})^m$ is dominated

by the n^m computations of the supercharacter values. Even for modest choices of n and even if $m = 2$, the amount of time needed to generate these plots can get out of hand quite quickly.

Because of this, we are often quite limited in the choices of modulus with which we are allowed to experiment. Thus, it is often good practice to construct n oneself by choosing the primes in its factorization. This allows one to guarantee the existence of elements in the automorphism group which have the desired properties.

In particular, one property that one might wish to control is an element's multiplicative order, which—as we have seen—is often the most important attribute when studying Gaussian periods and their analogues. Thus, in order to facilitate the work of an interested reader, we offer a few basic observations that might be useful if one hasn't worked much with these groups before.

- All the automorphism groups arising in the study of Gaussian periods and the cyclic supercharacters described in Chapters 2 and 3 are isomorphic to $\mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ for some $n \geq 2$ and $m \geq 1$. If $n = p_1^{e_1} \cdots p_\ell^{e_\ell}$ is the factorization into prime powers, then one can use the Chinese Remainder Theorem to decompose this group as

$$\mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z}) \cong \mathrm{GL}_m(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times \mathrm{GL}_m(\mathbb{Z}/p_\ell^{e_\ell}\mathbb{Z}).$$

  Additionally, if p^e is some prime power, then we have that

$$\#\mathrm{GL}_m(\mathbb{Z}/p^e\mathbb{Z}) = p^{(e-1)m^2}(p^m - 1)(p^m - p)\cdots(p^m - p^{m-1}).$$

  Thus if d is the order of some element $A \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$, then d must divide

$$\prod_{i=1}^{\ell} p_i^{(e_i-1)m^2}(p_i^m - 1)\cdots(p_i^m - p_i^{m-1}).$$

- Finding an element $A \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ such that $\Phi_d(A) = 0 \bmod n$ is often laborious, and we haven't found a method much better than simply having Sage do the following:

  (i) Take a matrix $A \in \mathrm{Mat}_m(\mathbb{Z}/n\mathbb{Z})$.

  (ii) Verify that $\det(A)$ is relatively prime to n. If not, go back to (i).

  (iii) Compute the multiplicative order of A mod n.

  (iv) If the order from (iii) is not d, go back to (i).

  (v) If the order from (iii) is d, compute $\Phi_d(A)$ mod n. If this is $0 \in \mathrm{Mat}_m(\mathbb{Z}/n\mathbb{Z})$, then return A. Otherwise, go back to (i).

  However, we have noticed that such an element seems to exist in $\mathrm{GL}_m(\mathbb{Z}/p^e\mathbb{Z})$ only when d divides $\#\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$. Thus, such an element should exist in $\mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ only when $d \mid (\#\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z}))$ for every $p \mid n$. The converse is not necessarily true, since (for example) one can verify computationally that there is no $A \in \mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z})$ which satisfies Φ_5.

- Otherwise, when trying to find an element $A \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ of order d that doesn't need to satisfy Φ_d, we often found it to be faster simply to find the order of some random matrix B (say the order is c), and if d divides c, then we set $A = B^{c/d}$.

- When trying to find elements $A \in \mathrm{GL}_m(\mathbb{Z}/p^e\mathbb{Z})$ of order p^a (that don't need to satisfy Φ_{p^a}), one can verify (using the Binomial Theorem) that if $B \in \mathrm{Mat}_m(\mathbb{Z}/p^a\mathbb{Z})$ and the matrix $A = I + p^{e-a}B$ is invertible, then A will have order dividing p^a. When $m = 1$, we can be more explicit: an element $\omega \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ has order p^a if and only if $\omega = 1 + p^{e-a}\beta$ for some $\beta \in (\mathbb{Z}/p^a\mathbb{Z})^\times$.

CHAPTER 4

CLASS FIELD THEORY PERSPECTIVE

The work presented in this chapter includes and expands upon [Pla24, §4], which is set to appear in the *International Journal of Number Theory*.

We now step away from supercharacter theory and return to Gaussian periods, this time viewing them from the perspective of class field theory. As a reminder, we stated in Section 1.6 that the ray class field for $\mathbb{Q}$ of modulus $(n) \subseteq \mathbb{Z}$ is the cyclotomic field $\mathbb{Q}(\mu_n)$, where $\mu_n \subseteq \mathbb{C}^\times$ is the subset of n-th roots of unity. The ray class group of modulus (n) is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, and from $\omega \in (\mathbb{Z}/n\mathbb{Z})^\times$ we get a cyclic subgroup $\langle\omega\rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$. From this perspective, Gaussian periods correspond to elements that generate the subfield $\mathbb{Q}(\mu_n)^{\langle\omega\rangle} \subseteq \mathbb{Q}(\mu_n)$ fixed by the action of this subgroup.

Now, this is the whole story for the rational field $\mathbb{Q}$, but we would like to generalize this to other base fields. Ostensibly, this story is simple enough to recreate. Take a number field K, an ideal $\mathfrak{m} \subseteq \mathcal{O}_K$, its ray class field $K[\mathfrak{m}]$ of modulus $\mathfrak{m}$, and its ray class group $Cl_K(\mathfrak{m})$. Choose an element $\omega \in Cl_K(\mathfrak{m})$, and sum over the Galois action of $\langle\omega\rangle$ to obtain generators of the subfield $K[\mathfrak{m}]^{\langle\omega\rangle}$. However, in order to recreate this story *explicitly*, one needs to have explicit elements of the ray class field $K[\mathfrak{m}]$. As stated in Section 1.6, this is a problem to which we have very few answers.

As of the writing of this dissertation, there are two main classes of fields other than $\mathbb{Q}$ for which we have explicit descriptions of their ray class fields. The first is quadratic imaginary fields (fields of the form $\mathbb{Q}(\sqrt{-D})$ for positive square-free D), where the theory of complex multiplication provides an answer. The second is the much more recent case of totally real fields, in which Dasgupta and Kakde showed

in [DK23] that the ray class fields can be generated using Brumer-Stark units and square roots of certain elements of of the base field.

For the rest of this chapter, we will explore the case of quadratic imaginary fields, starting with an overview of elliptic curves and the theory of complex multiplication. For further reading on elliptic curves and complex multiplication, we recommend [Sil86] and [Sil94, Chapter II].

4.1 Elliptic Curves and Complex Multiplication

Our goal in this section is to describe the construction of ray class fields of quadratic imaginary fields, along with some useful related theorems. We start with some basic definitions.

Definition 4.1. An *elliptic curve* over $\mathbb{C}$ is the set of solutions $(x, y) \in \mathbb{C}^2$ to the following equation:

$$y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{C}$. An elliptic curve E over $\mathbb{C}$ has a natural group structure, where the identity element is the point at infinity $[0, 1, 0]$ (when viewing E as a subset of projective space $\mathbb{P}^2$).

From now on, our elliptic curves will only be over $\mathbb{C}$, so we will often drop this qualifier.

Definition 4.2. Let E be an elliptic curve. An *endomorphism* of E is a group homomorphism $\phi : E \to E$. The set $\mathrm{End}(E)$ of endomorphisms of E form a ring under pointwise addition and function composition.

Proposition 4.3 (Proposition III.4.2 in [Sil86])**.** *For any elliptic curve E and any $m \in \mathbb{Z}$, there exists a multiplication-by-m endomorphism $[m] : E \to E$. Thus $\mathbb{Z} \subseteq End(E)$ for all E.*

In most cases, these multiplication-by-m maps describe all of $\mathrm{End}(E)$. However, the situations where $\mathbb{Z} \neq \mathrm{End}(E)$ (that is, when $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$) will be of particular interest to us. Before getting there, however, we need a couple of definitions.

Definition 4.4. Let V be a vector space of dimension n over $\mathbb{R}$, and let $e_1, \ldots, e_r$ be linearly independent vectors over $\mathbb{R}$. Then a *lattice* is a subgroup

$$\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r.$$

In the case when $r = n$, we call Λ a *full lattice*.

Proposition 4.5. *Every full lattice $\Lambda \subseteq \mathbb{C}$ can be written as $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ for some τ in the complex upper half-plane*

$$\mathcal{H} = \{z \in \mathbb{C} : Im(z) > 0\}.$$

Definition 4.6. Let R be a ring. An *order* $\mathcal{O}$ is a subring of R such that the following hold:

- $\mathcal{O}$ is a finite-dimensional algebra over $\mathbb{Q}$
- R is spanned by $\mathcal{O}$ over $\mathbb{Q}$
- $\mathcal{O}$ is a $\mathbb{Z}$-lattice in R.

We are now ready to discuss the case when $\mathrm{End}(E) \neq \mathbb{Z}$.

Definition 4.7. Let E be an elliptic curve. Then E is said to have *complex multiplication* (shortened to CM) if $\mathrm{End}(E)$ is isomorphic to a quadratic imaginary order $\mathcal{O}$. That is, $\mathrm{End}(E)$ is an order in some quadratic imaginary field K over $\mathbb{Q}$. If $\mathcal{O}$ is contained in the quadratic imaginary field K, then we say that E has CM by K.

Elliptic curves with CM have many special properties. For our purposes, however, we focus only on the relationship between CM and abelian extensions of quadratic imaginary fields.

Proposition 4.8 (Proposition II.1.2 in [Sil94])**.** *Let K be a quadratic imaginary field. Let $\mathcal{E}(K)$ denote the set of elliptic curves with CM by K, up to isomorphism. Then $\mathcal{E}(K)$ is finite, and there exists a bijection between $\mathcal{E}(K)$ and the ideal class group $Cl_K(1)$.*

Recall that the Hilbert class field $K[1]$ has degree $[K[1] : K] = \#Cl_K(1)$ over K. We will be using the fact that there is a bijection between $Cl_K(1)$ and $\mathcal{E}(K)$ to obtain generators of the Hilbert class field, but before we can do that, we must first describe a different characterization of elliptic curves over $\mathbb{C}$, which requires the following definition.

Definition 4.9. Two full lattices Λ_1 and Λ_2 in $\mathbb{C}$ are called *homothetic* if there exists $\alpha \in \mathbb{C}^\times$ such that $\Lambda_1 = \alpha\Lambda_2$.

Using this definition, we can now characterize elliptic curves using lattices.

Theorem 4.10 (Uniformization Theorem)**.** *Let E be an elliptic curve over $\mathbb{C}$. Then there exists a $\mathbb{Z}$-lattice $\Lambda \subseteq \mathbb{C}$, unique up to homothety, such that E is isomorphic to $\mathbb{C}/\Lambda$ via the complex analytic isomorphism*

$$\phi : \mathbb{C}/\Lambda \to E, \qquad \phi(z) = (\wp(z;\Lambda), \wp'(z;\Lambda)),$$

where $\wp$ is the Weierstrass $\wp$-function defined to be the following:

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right).$$

The Weierstrass $\wp$-function will be important to us later for computational purposes, but for now we focus on the fact that choosing an elliptic curve (up to isomorphism) is equivalent to choosing a lattice $\Lambda \subseteq \mathbb{C}$ (up to homothety). With this fact, we are now ready to describe how to obtain the generators of the Hilbert class fields of quadratic imaginary fields.

Theorem 4.11 (Theorems II.4.1 and II.4.3 in [Sil94])**.** *Let K be a quadratic imaginary field. Let $E_1, \ldots, E_\ell$ be representatives of all the isomorphism classes of elliptic curves with CM by K. Let $\Lambda_1, \ldots, \Lambda_\ell$ be the lattices in $\mathbb{C}$ such that $E_i \cong \mathbb{C}/\Lambda_i$, and write $\Lambda_i = \mathbb{Z} + \mathbb{Z}\tau_i$, where τ_i is in the upper half-plane. There exists a weight 0 modular function j such that the Hilbert class field $K[1]$ is achieved by adjoining the values $j(\tau_1), \ldots, j(\tau_\ell)$. In fact, the $j(\tau_i)$ are all algebraic conjugates, so*

$$K[1] = K(j(\tau_i))$$

for any choice of $i \in \{1, \ldots, \ell\}$.

To clarify the sort of object that the function j is, we provide the following definition.

Definition 4.12. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and let $\mathcal{H}$ be the complex upper half-plane. For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $z \in \mathcal{H}$, there exists a natural action

$$\gamma \cdot z = \frac{az+b}{cz+d}.$$

For an integer k, we say that a function $f : \mathcal{H} \to \mathbb{C}$ is a *modular function of weight k* if the following conditions hold:

- f is a meromorphic function
- For all $\gamma \in \Gamma$, we have $f(\gamma \cdot z) = (cz + d)^k f(z)$
- $f(z)$ is bounded as $\mathrm{Im}(z) \to \infty$.

Since the function j is a modular function of weight 0, then $j(\gamma \cdot \tau) = j(\tau)$ for all $\gamma \in \Gamma$ and $\tau \in \mathcal{H}$.

Remark 4.13. It is common to abuse notation for the function j by allowing elliptic curves as inputs rather than elements of the upper half-plane. That is, if E is an elliptic curve which is isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subseteq \mathbb{C}$, then we understand $j(E)$ to mean $j(\tau)$, where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ with τ in the upper half-plane. In this way, we can write the result of the theorem above as saying that $K[1] = K(j(E))$, where E is any elliptic curve with CM by K.

Recall that the Hilbert class field $K[1]$ is the maximal abelian extension of K which is unramified at every prime of K. The above theorem allows us to construct explicitly the Hilbert class fields of quadratic imaginary fields; however, to construct abelian extensions where ramification at certain primes is allowed, we require the following definitions.

Definition 4.14. Let E be an elliptic curve with CM by a quadratic imaginary field K. Let $\mathfrak{m} \subseteq \mathcal{O}_K$ be an ideal. We define the $\mathfrak{m}$-*torsion subgroup of* E to be

$$E[\mathfrak{m}] = \{t \in E : [\alpha] \cdot t = 0 \text{ for every } \alpha \in \mathfrak{m}\},$$

where 0 represents the identity element of E, and $[\alpha] \cdot t$ represents the normalized action of α on t as an element of $\mathrm{End}(E)$ (as mentioned in [Sil94, Prop II.1.1]).

Remark 4.15. Note that in the special case that $\mathfrak{m} = (m)$ for $m \in \mathbb{Z}$, then

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

due to the fact that $E \cong \mathbb{C}/\Lambda$.

Definition 4.16. Let E be an elliptic curve with CM by a quadratic imaginary field K. Suppose E is defined by the equation $y^2 = x^3 + Ax + B$. Then a *Weber function* is a finite map $h : E \to E/\mathrm{Aut}(E)$. For our purposes, we follow the convention of [Sil94, II.5.5.1] and use the following Weber function:

$$h(x,y) = \begin{cases} x & AB \neq 0, \\ x^2 & B = 0, \\ x^3 & A = 0. \end{cases}$$

Remark 4.17. The two special cases of $A = 0$ and $B = 0$ correspond to the cases where E has CM by $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-1})$, respectively. These are the only quadratic imaginary fields which contain roots of unity other than -1 and 1 (i.e. where $\mathrm{Aut}(E)$ is strictly larger than $\{\pm 1\}$), and it is for this reason that their Weber functions are different. In most cases, however, note that the Weber function is simply projection to the x-coordinate.

We now use all of this to construct the ray class fields of quadratic imaginary fields.

Theorem 4.18 (Theorem II.5.6 of [Sil94])**.** *Let K be a quadratic imaginary field with ring of integers $\mathcal{O}_K$, let $\mathfrak{m} \subseteq \mathcal{O}_K$ be an ideal, let E be an elliptic curve with CM by K, and let $h : E \to E/Aut(E)$ be a Weber function. Then the field*

$$K(j(E), h(E[\mathfrak{m}]))$$

is the ray class field of K of modulus $\mathfrak{m}$.

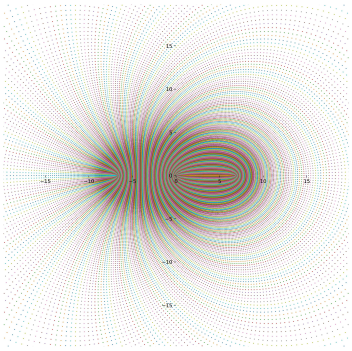
Remark 4.19. The result of the above theorem can be stated in the following way. Start with a quadratic imaginary field K, a modulus $\mathfrak{m} \subseteq \mathcal{O}_K$, and an elliptic curve

E with CM by K. In order to obtain the ray class field $K[\mathfrak{m}]$, one must first adjoin $j(E)$ to K, followed by adjoining the x-coordinates of the $\mathfrak{m}$-torsion points of E (or the squares of x-coordinates for $K = \mathbb{Q}(\sqrt{-1})$, the cubes for $K = \mathbb{Q}(\sqrt{-3})$). Thus the roots of unity for $\mathbb{Q}$ are analogous to certain j-values and certain coordinates of elliptic curve torsion points for a quadratic imaginary field K.

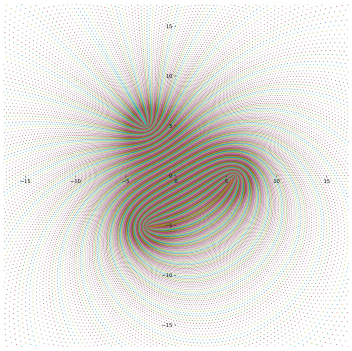
To continue the last point of Remark 4.19, we note that the roots of unity are quite simple to describe geometrically, as they are simply points lying on the unit circle in $\mathbb{C}$. However, the j-values and $\mathfrak{m}$-torsion points of elliptic curves are more complicated to describe geometrically.

In fact, to the author's knowledge, it seems that there hasn't been much study of elliptic curve torsion points from a graphical perspective. One reason for this might be that elliptic curves inherently live in a four-dimensional $\mathbb{R}$-vector space, which are notoriously difficult to represent graphically (to say the least). However, our study will focus almost exclusively on the x-coordinates (which live in $\mathbb{C}$), so we thought it might be of interest to generate images of the x- and y-coordinates of elliptic curve torsion points in the complex plane.

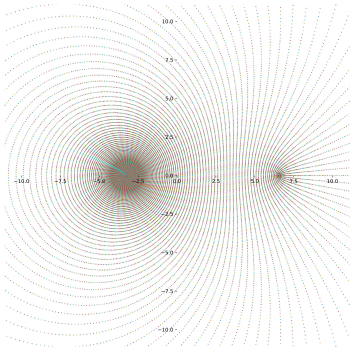
To this end, we offer examples of these images in Figure 4.1 and Figure 4.2. The images in Figure 4.1 have no special properties other than their coloring, which is simply the coloring that Python automatically applies to scatter plots (it cycles through a list of colors). The images in Figure 4.2 take inspiration from [HST22], in which we size the torsion points inversely based on their additive order in the torsion group; that is, the smaller the order of the torsion point, the larger the dot. We discuss our computational methods for these images and others (including how we chose the elliptic curves with CM) after the proof of Proposition 4.20 in the next section.



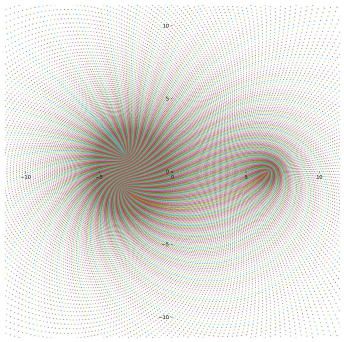
(a) x-coordinates, $K = \mathbb{Q}(\sqrt{-1})$



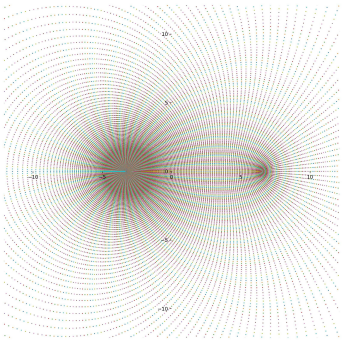
(b) x-coordinates, $K = \mathbb{Q}(\sqrt{-3})$



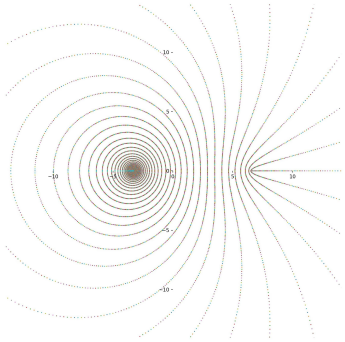
(c) x-coordinates, $K = \mathbb{Q}(\sqrt{-43})$



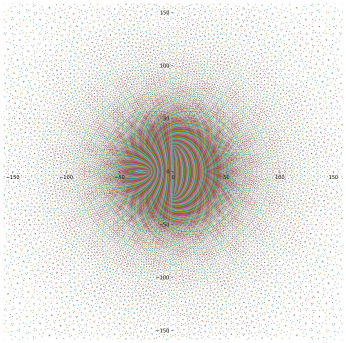
(d) x-coordinates, $K = \mathbb{Q}(\sqrt{-7})$



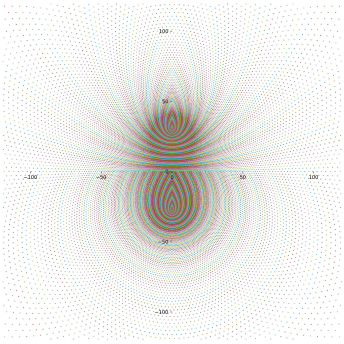
(e) x-coordinates, $K = \mathbb{Q}(\sqrt{-5})$



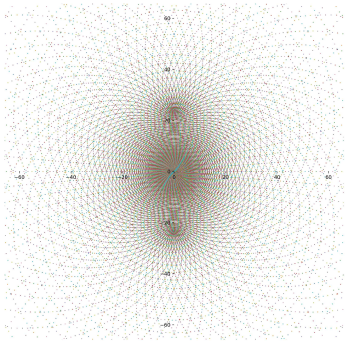
(f) x-coordinates, $K = \mathbb{Q}(\sqrt{-101})$



(g) y-coordinates, $K = \mathbb{Q}(\sqrt{-1})$

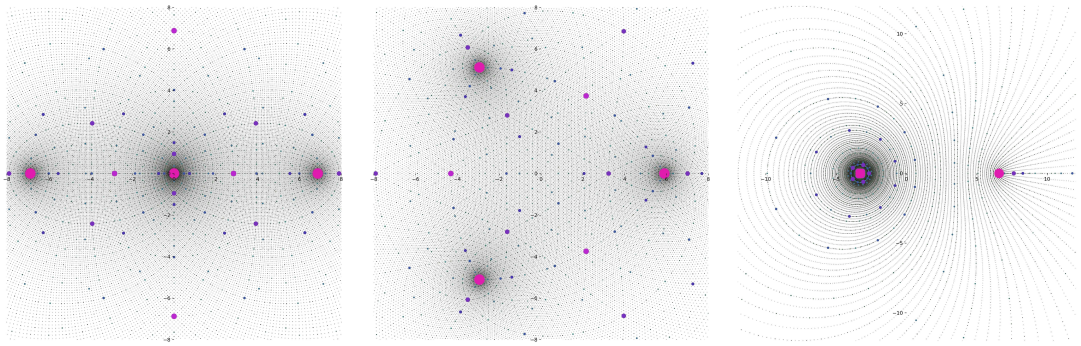


(h) y-coordinates, $K = \mathbb{Q}(\sqrt{-3})$

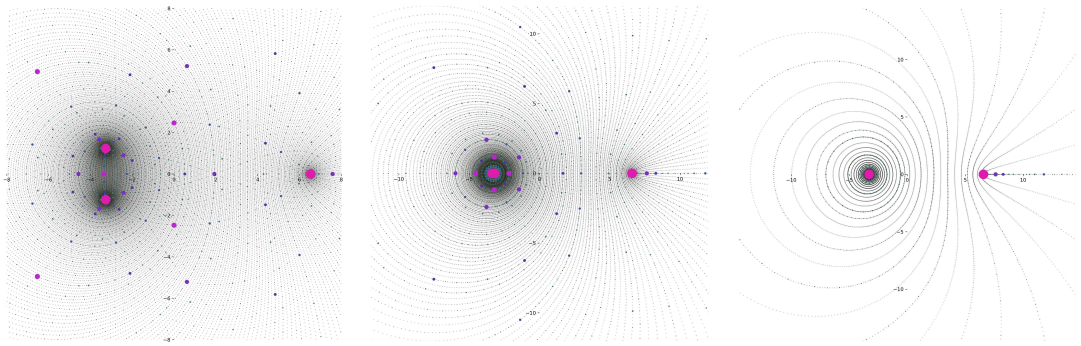


(i) y-coordinates, $K = \mathbb{Q}(\sqrt{-43})$

Figure 4.1. Coordinates of 400-torsion points of elliptic curves $E \cong \mathbb{C}/\mathcal{O}_K$



(a) $K = \mathbb{Q}(\sqrt{-1})$ *(b)* $K = \mathbb{Q}(\sqrt{-3})$ *(c)* $K = \mathbb{Q}(\sqrt{-43})$



(d) $K = \mathbb{Q}(\sqrt{-7})$ *(e)* $K = \mathbb{Q}(\sqrt{-5})$ *(f)* $K = \mathbb{Q}(\sqrt{-101})$

Figure 4.2. x-coordinates of 400-torsion points of elliptic curves $E \cong \mathbb{C}/\mathcal{O}_K$, where dots are sized inversely according to their order in $E[m]$

4.2 The Galois Group and Its Action

We are now able to explicitly compute the generators of the ray class fields of modulus $\mathfrak{m}$ for quadratic imaginary fields K. Our goal now is to compute the ray class group of modulus $\mathfrak{m}$ for the quadratic imaginary field K and to describe its Galois action on the ray class field.

In actuality, however, we won't be computing the full ray class group $Cl_K(\mathfrak{m})$. Recall that the ideal class group $Cl_K(1)$ is contained in $Cl_K(\mathfrak{m})$ for any modulus $\mathfrak{m}$. Thus, in order to compute the full ray class group of modulus $\mathfrak{m}$, we also need

to compute the ideal class group for any quadratic imaginary field K. This part of the computation can be rather complex, and its difficulty depends on the base field. That is, computing the full group $Cl_K(\mathfrak{m}) \cong \mathrm{Gal}(K[\mathfrak{m}]/K)$ can be quite difficult.

However, the field extension $K[1] \subseteq K[\mathfrak{m}]$ is much more predictable, and computing the subgroup $\mathrm{Gal}(K[\mathfrak{m}]/K[1])$ proves to be more straightforward using class field theory. This extension also contains a lot of the number theoretic information that we're interested in anyway; for example, the analogous extension $\mathbb{Q} \subseteq \mathbb{Q}(\mu_n)$ famously holds a plethora of important number theoretic information.

Thus, for our purposes, we will restrict ourselves to studying the extension $K[1] \subseteq K[\mathfrak{m}]$ and its Galois group $\mathrm{Gal}(K[\mathfrak{m}]/K[1])$. The following proposition describes the structure of this group.

Proposition 4.20 (Proposition 33 of [Pla24])**.** *Let $K = \mathbb{Q}(\sqrt{-D})$ be a quadratic imaginary field and $\mathfrak{m} \subseteq \mathcal{O}_K$ an ideal. Let $K[\mathfrak{m}]$ be the ray class field for K of modulus $\mathfrak{m}$, and let $K[1]$ be its Hilbert class field. Let ρ be a primitive third root of unity. Then the field extension $K[1] \subseteq K[\mathfrak{m}]$ has Galois group*

$$Gal(K[\mathfrak{m}]/K[1]) \cong {(\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times}\big/{\mathcal{O}_K^\times},$$

where $\mathcal{O}_K^\times$ is the cyclic multiplicative group $\{\pm 1, \pm i\}$ when $D = 1$, $\{\pm 1, \pm\rho, \pm\bar{\rho}\}$ when $D = 3$, and $\{\pm 1\}$ otherwise.

We note that while the result of this proposition seems to be known by those who use class field theory regularly, it is only scarcely mentioned explicitly in the literature. Because of this, we have decided to include a proof. This proof requires some knowledge of certain class field theoretic objects and ideas (the idèles and the Artin map for example). However, it's not required to know the details of this proof to understand the rest of this chapter, so we leave the choice to the reader on how to proceed.

Proof. Let $\mathbb{A}_K^\times$ be the group of idèles. Given a modulus $\mathfrak{m}$, define the open normal subgroup

$$U_\mathfrak{m} := \mathbb{C}^\times \cdot \prod_{v<\infty, v\nmid\mathfrak{m}} \mathcal{O}_{K,v}^\times \cdot \prod_{v<\infty, v\mid\mathfrak{m}} (1+\mathfrak{p}_v^{\mathrm{ord}_v(\mathfrak{m})}\mathcal{O}_{K,v}),$$

where $\mathcal{O}_{K,v}$ is the completion of $\mathcal{O}_K$ with respect to the place v and where $\mathfrak{p}_v$ is the prime ideal corresponding to the place v. Then using class field theory, we know that $\mathrm{Gal}(K[\mathfrak{m}]/K) \cong {}^{\mathbb{A}_K^\times}\!/_{U_\mathfrak{m}K^\times}$. Similarly, we know that $\mathrm{Gal}(K[1]/K) \cong {}^{\mathbb{A}_K^\times}\!/_{U_1K^\times}$.

By Galois theory, the group $\mathrm{Gal}(K[\mathfrak{m}]/K[1])$ is a subgroup of $\mathrm{Gal}(K[\mathfrak{m}]/K)$, and we have the isomorphism

$$\mathrm{Gal}(K[1]/K) \cong {}^{\mathrm{Gal}(K[\mathfrak{m}]/K)}\!/_{\mathrm{Gal}(K[\mathfrak{m}]/K[1])}.$$

This isomorphism is induced by the surjective homomorphism

$$\varphi : \mathrm{Gal}(K[\mathfrak{m}]/K) \twoheadrightarrow \mathrm{Gal}(K[1]/K), \qquad \sigma \mapsto \sigma|_{K[1]},$$

whose kernel is isomorphic to $\mathrm{Gal}(K[\mathfrak{m}]/K[1])$.

This homomorphism can be described idèlically in the following way:

$$\psi : {}^{\mathbb{A}_K^\times}\!/_{U_\mathfrak{m}K^\times} \to {}^{\mathbb{A}_K^\times}\!/_{U_1K^\times}, \qquad (a_v)_v + U_\mathfrak{m}K^\times \mapsto (a_v)_v + U_1K^\times.$$

Note that $U_\mathfrak{m} \subseteq U_1$, so this map is surjective. The elements of $\ker(\psi)$ are cosets of $U_\mathfrak{m}K^\times$ which are contained in $U_1K^\times$, and so $\ker(\psi) \cong {}^{U_1K^\times}\!/_{U_\mathfrak{m}K^\times}$. Additionally, the isomorphisms ${}^{\mathbb{A}_K^\times}\!/_{U_\mathfrak{m}K^\times} \cong \mathrm{Gal}(K[\mathfrak{m}]/K)$ and ${}^{\mathbb{A}_K^\times}\!/_{U_1K^\times} \cong \mathrm{Gal}(K[1]/K)$ are given by the Artin map. By a slight abuse of notation, we denote both Artin maps by ϕ. Then we have the following diagram:

$$\begin{array}{ccc} {}^{\mathbb{A}_K^\times}\!/_{U_\mathfrak{m}K^\times} & \xrightarrow{\ \psi\ } & {}^{\mathbb{A}_K^\times}\!/_{U_1K^\times} \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ \mathrm{Gal}(K[\mathfrak{m}]/K) & \xrightarrow{\ \varphi\ } & \mathrm{Gal}(K[1]/K) \end{array}$$

Note that the elements of $\phi\left({}^{U_1K^\times}\!/_{U_\mathfrak{m}K^\times}\right)$ are precisely the elements of $\mathrm{Gal}(K[\mathfrak{m}]/K)$ which act nontrivially on $K[\mathfrak{m}]$, but trivially on $K[1]$. In other words, we have that

$$\phi\left({}^{U_1K^\times}\!/_{U_\mathfrak{m}K^\times}\right) = \ker(\varphi).$$

This shows that the diagram above is commutative, which induces the following isomorphism:

$$\mathrm{Gal}(K[\mathfrak{m}]/K[1]) \cong {}^{U_1K^\times}\!/_{U_\mathfrak{m}K^\times},$$

where this uses the fact that $\ker(\varphi) \cong \mathrm{Gal}(K[\mathfrak{m}]/K[1])$.

In the interest of computing the group ${}^{U_1K^\times}\!/_{U_\mathfrak{m}K^\times}$ explicitly, we let $G = U_1$ and $H = U_\mathfrak{m}K^\times$. Then ${}^{U_1K^\times}\!/_{U_\mathfrak{m}K^\times} = {}^{GH}\!/_{H}$, and by the second isomorphism theorem we have that

$${}^{GH}\!/_{H} \cong {}^{G}\!/_{(G \cap H)}.$$

Note that $G \cap H = U_1 \cap (U_\mathfrak{m}K^\times)$. An element of $U_\mathfrak{m}K^\times$ is of the form $(a_v\alpha)_v$ for $(a_v)_v \in U_\mathfrak{m}$ and $\alpha \in K^\times$. If this element is also in $U_1 = \mathbb{C}^\times \cdot \prod_{v<\infty} \mathcal{O}_{K,v}^\times$, then α must be in $\mathcal{O}_{K,v}^\times$ for every finite place v. This happens if and only if $\mathrm{ord}_v(\alpha) = 0$ for every finite place v, so α must be an element of $\mathcal{O}_K^\times$. Then, since $U_\mathfrak{m} \subseteq U_1$, we have that $U_1 \cap (U_\mathfrak{m}K^\times) = U_\mathfrak{m}\mathcal{O}_K^\times$. Thus we have the following:

$${}^{U_1K^\times}\!/_{U_\mathfrak{m}K^\times} \cong {}^{U_1}\!/_{(U_1 \cap (U_\mathfrak{m}K^\times))} = {}^{U_1}\!/_{U_\mathfrak{m}\mathcal{O}_K^\times}.$$

Using the definitions of U_1 and $U_\mathfrak{m}$, the quotient ${}^{U_1}\!/_{U_\mathfrak{m}\mathcal{O}_K^\times}$ reduces to the following:

$${}^{U_1}\!/_{U_\mathfrak{m}\mathcal{O}_K^\times} \cong \prod_{v<\infty, v|\mathfrak{m}} {}^{\mathcal{O}_{K,v}^\times}\!/ \prod_{v<\infty, v|\mathfrak{m}} (1 + \mathfrak{p}_v^{\mathrm{ord}_v(\mathfrak{m})}\mathcal{O}_{K,v})\mathcal{O}_K^\times.$$

By the Chinese Remainder Theorem, we need only compute ${}^{\mathcal{O}_{K,v}^\times}\!/_{(1 + \mathfrak{p}_v^{\mathrm{ord}_v(\mathfrak{m})}\mathcal{O}_{K,v})}$ for each place $v \mid \mathfrak{m}$.

For a fixed place v and a fixed $k \in \mathbb{N}$, we construct a map

$$f : \mathcal{O}_{K,v}^{\times} \to \left(\mathcal{O}_{K,v}/\mathfrak{p}_v^k \mathcal{O}_{K,v}\right)^{\times}$$

sending a unit $u \mapsto u \bmod \mathfrak{p}_v^k$. This is a homomorphism, and we claim it is surjective. To see this, let $u \in \left(\mathcal{O}_{K,v}/\mathfrak{p}_v^k \mathcal{O}_{K,v}\right)^{\times}$. Then we have

$$u = a_0 + a_1\pi + \cdots + a_{k-1}\pi^{k-1},$$

where π is a uniformizer of $\mathfrak{p}_v$, $a_i \in \mathcal{O}_{K,v}/\mathfrak{p}_v \mathcal{O}_{K,v}$ for all i, and $a_0 \neq 0$ (a_0 cannot be 0 because u is a unit). Then, since $a_0 \neq 0$, there exists an element $\tilde{u} \in \mathcal{O}_{K,v}^{\times}$ such that $\tilde{u} = a_0 + a_1\pi + \cdots + a_{k-1}\pi^{k-1} + \cdots$. Thus for any $u \in \left(\mathcal{O}_{K,v}/\mathfrak{p}_v^k \mathcal{O}_{K,v}\right)^{\times}$, there exists $\tilde{u} \in \mathcal{O}_{K,v}^{\times}$ such that $f(\tilde{u}) = u$.

Now, note that the kernel of f is any element $u \in \mathcal{O}_{K,v}^{\times}$ such that $u \equiv 1 \bmod \mathfrak{p}_v^k$. That is, the element $u \in \ker(f)$ if and only if $u \in (1+\mathfrak{p}_v^k \mathcal{O}_{K,v})$. Thus the surjectivity of f induces the following isomorphism:

$$\mathcal{O}_{K,v}^{\times}/(1 + \mathfrak{p}_v^k \mathcal{O}_{K,v}) \cong \left(\mathcal{O}_{K,v}/\mathfrak{p}_v^k \mathcal{O}_{K,v}\right)^{\times}.$$

By a well-known fact about completions, we also have that

$$\left(\mathcal{O}_{K,v}/\mathfrak{p}_v^k \mathcal{O}_{K,v}\right)^{\times} \cong \left(\mathcal{O}_K/\mathfrak{p}_v^k \mathcal{O}_K\right)^{\times}.$$

Thus we have the following:

$$\begin{aligned} U_1/U_{\mathfrak{m}}\mathcal{O}_K^{\times} &\cong \prod_{v<\infty, v|\mathfrak{m}} \mathcal{O}_{K,v}^{\times} / \prod_{v<\infty, v|\mathfrak{m}} (1 + \mathfrak{p}_v^{\mathrm{ord}_v(\mathfrak{m})}\mathcal{O}_{K,v})\mathcal{O}_K^{\times} \\ &\cong (\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^{\times}/\mathcal{O}_K^{\times}, \end{aligned}$$

where the last equality comes from reversing the direction of the Chinese Remainder Theorem. □

Now that we know the structure of $\mathrm{Gal}(K[\mathfrak{m}]/K[1])$, we need to determine its action on $K[\mathfrak{m}]$. Since $K[\mathfrak{m}] = K(j(E), h(E[\mathfrak{m}]))$ and $K[1] = K(j(E))$, then the action of $\mathrm{Gal}(K[\mathfrak{m}]/K[1])$ on $K[\mathfrak{m}]$ permutes only the elliptic curve torsion points and leaves the j-values fixed. In other words, we want to determine the action of $(\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times \,/\, \mathcal{O}_K^\times$ on the set $h(E[\mathfrak{m}])$.

We first need an elliptic curve with CM by K. Recall that choosing an elliptic curve is equivalent to choosing a lattice in $\mathbb{C}$ by the Uniformization Theorem, so the simplest way to choose an elliptic curve with CM by K is to choose the lattice $\Lambda = \mathcal{O}_K$. This lattice will automatically be closed under multiplication by elements of $\mathcal{O}_K$, so $\mathbb{C}/\mathcal{O}_K$ will have CM by K.

For our purposes, however, we need to be more explicit. For $K = \mathbb{Q}(\sqrt{-D})$, we use the lattice $\Lambda := \mathbb{Z} + \mathbb{Z}\alpha$, where $\alpha \in \mathcal{O}_K$ is chosen in the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ to be the following:

$$\alpha = \begin{cases} \sqrt{-D} & D \equiv 1, 2 \bmod 4, \\ \frac{-1+\sqrt{-D}}{2} & D \equiv 3 \bmod 4. \end{cases}$$

Note that in the second case, we could have equivalently chosen $\alpha = \frac{1+\sqrt{-D}}{2}$. We chose this definition so that α is a third root of unity in the case $D = 3$.

Thus we now have an elliptic curve $E \cong \mathbb{C}/\Lambda$ which has CM by K. Note that a point (x, y) on our elliptic curve can be found via the Uniformization Theorem by taking a complex number $z \in \mathbb{C}/\Lambda$ and using the Weierstrass $\wp$-function to get $x = \wp(z; \Lambda)$ and $y = \wp'(z; \Lambda)$. Because of this, we will use $\mathbb{C}/\Lambda$ for the majority of our calculations, as computations are much simpler in this setting when compared to viewing E as a subset of $\mathbb{P}^2$, even though the latter viewpoint is the one needed in the end.

Additionally, we will restrict our attention to the case in which $\mathfrak{m} = (m)$ is

an ideal generated by an integer. The analogy of Gaussian periods we define in the next section allows for any integral ideal $\mathfrak{m}$, but for the time being, it is more intuitive and insightful to discuss only the $\mathfrak{m} = (m)$ case.

To determine the m-torsion points of E, we must find the complex numbers z such that $mz \in \Lambda$. If we restrict z to the fundamental parallelogram, then an m-torsion point z must be of the form $z = \frac{1}{m}(a + b\alpha)$, where $a, b \in \{0, 1, \ldots, m-1\}$. This gives all m^2 of the m-torsion points, matching the statement of Remark 4.15.

We now define the Galois action. Let $\beta \in (\mathcal{O}_K/m\mathcal{O}_K)^\times/\mathcal{O}_K^\times$, so we can write $\beta = c + d\alpha$ for $c, d \in \mathbb{Z}/m\mathbb{Z}$. Let $\rho \in h(E[m])$; that is, ρ is an element of $K[m]$ but not $K[1]$. Since ρ is a power of the x-coordinate of an m-torsion point of E, then there exist $a, b \in \mathbb{Z}/m\mathbb{Z}$ and a power $e \in \{1, 2, 3\}$ (depending on the base field) such that $z = \frac{1}{m}(a + b\alpha)$ and $\rho = \wp(z; \Lambda)^e$. The Galois action of β on ρ is given by

$$\beta \cdot \rho = \wp(\beta z; \Lambda)^e,$$

where βz is the standard multiplication of complex numbers.

Remark 4.21. For computational purposes, it is best if we view z and β as matrices in $\mathrm{Mat}_2(\mathbb{Z}/m\mathbb{Z})$, where we represent α with the companion matrix of its minimal polynomial. More explicitly, we use the matrix

$$C_\alpha = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & -D \end{pmatrix} & D \equiv 1, 2 \bmod 4, \\ \begin{pmatrix} 1 & -\frac{D+1}{2} \\ 0 & -1 \end{pmatrix} & D \equiv 3 \bmod 4. \end{cases}$$

to represent α. Then we can view $\mathcal{O}_K/m\mathcal{O}_K$ as a subring embedded into $\mathrm{Mat}_2(\mathbb{Z}/m\mathbb{Z})$ via the map sending $\alpha \mapsto C_\alpha$ and $1 \mapsto I$. Thus an element $\gamma \in \mathcal{O}_K/m\mathcal{O}_K$ is given

by $\gamma = aI + bC_\alpha$ for some $a, b \in \mathbb{Z}/m\mathbb{Z}$. Additionally, the matrix γ is an element of $(\mathcal{O}_K/m\mathcal{O}_K)^\times$ if $\det(\gamma)$ is relatively prime to m.

4.3 Analogue Using Class Field Theory

In this section, we explicitly describe the analogue of Gaussian periods for quadratic imaginary fields, and we provide some examples of these analogues. We start with the definition.

Definition 4.22. Let K be a quadratic imaginary field, and choose $\alpha \in K$ so that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ as described in the previous section. Let $\Lambda = \mathbb{Z} + \mathbb{Z}\alpha$ and let E be the elliptic curve isomorphic to $\mathbb{C}/\Lambda$. Choose $A \in (\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times \,/\, \mathcal{O}_K^\times$, and let d denote the multiplicative order of A. Let $z \in \mathcal{O}_K/\mathfrak{m}\mathcal{O}_K$, represented as an element of $\mathbb{C}/\Lambda$, and let $\wp(z) := \wp(z;\Lambda)$ be the Weierstrass $\wp$-function. Then we define the following map:

$$\eta_{K,\mathfrak{m},A} : \mathcal{O}_K/\mathfrak{m}\mathcal{O}_K \to \mathbb{C}, \qquad \eta_{K,\mathfrak{m},A}(z) = \sum_{j=0}^{d-1} \wp(A^j z).$$

We call $\eta_{K,\mathfrak{m},A}(z)$ a *ray class field period (RCFP) for K of modulus $\mathfrak{m}$ and generator A*. Additionally, we call $\mathrm{img}(\eta_{K,\mathfrak{m},A})$ the *ray class field period plot (RCFP plot) for K of modulus $\mathfrak{m}$ and generator A*.

Remark 4.23. In the above definition, one can choose $A \in (\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times/\mathcal{O}_K^\times$ by first choosing an element $B \in (\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times$ and computing the cyclic subgroup $\langle B\rangle$. If $\langle B\rangle \cap \mathcal{O}_K^\times$ is not the trivial group, then one can choose A by taking B to an appropriate power. This sort of idea and others are discussed in Section 3.4.

Now, this definition of an ray class field period is specific to the context of quadratic imaginary fields. For any other base field K, we can still define an analogous definition; the issue is that we are unable to actually compute RCFPs for

base fields which don't have an answer to Hilbert's 12th problem. However, given a number field K that *does* have an answer to Hilbert's 12th problem, we have the following definition.

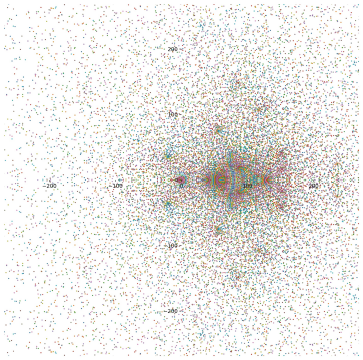
Definition 4.24. Let K be a number field, and let $\mathfrak{m} \subseteq \mathcal{O}_K$ be a modulus. Choose $A \in \mathrm{Gal}(K[\mathfrak{m}]/K[1])$, and let d denote the order of A in this group. For every $B \in \mathcal{O}_K/\mathfrak{m}\mathcal{O}_K$, let x_B denote the corresponding algebraic number in $K[\mathfrak{m}]$ over $K[1]$. Then we define the following map:

$$\eta_{K,\mathfrak{m},A} : \mathcal{O}_K/\mathfrak{m}\mathcal{O}_K \to \mathbb{C}, \qquad \eta_{K,\mathfrak{m},A}(B) = \sum_{j=0}^{d-1} A^j \cdot x_B,$$

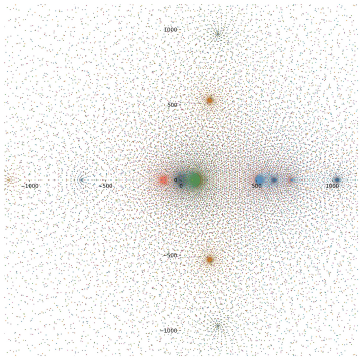
where $A^j \cdot x_B$ represents the Galois action of A^j on x_B. We call $\eta_{K,\mathfrak{m},A}(B)$ an *RCFP for K of modulus $\mathfrak{m}$ and generator A*. Additionally, we call $\mathrm{img}(\eta_{K,\mathfrak{m},A})$ the *RCFP plot for K of modulus $\mathfrak{m}$ and generator A*.

We now return to the case where K is a quadratic imaginary field. In Figure 4.3, we provide some examples of RCFP plots for various choices of fields $K = \mathbb{Q}(\sqrt{-D})$, ideals $\mathfrak{m} = (m)$, and elements A. Note that in these examples, we use fields with class number 1 to avoid entirely any nontrivial Hilbert class field and ideal class group.

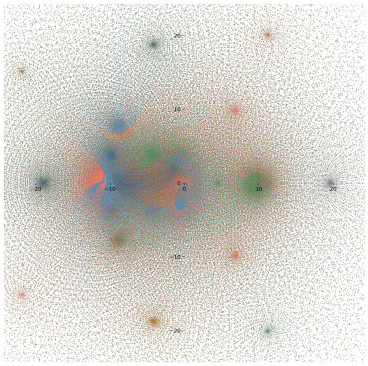
It should be noted that the scales for the real and imaginary axes vary in these images. The reason for doing this is because the values of $\wp$ vary largely for different choices of K, $\mathfrak{m}$, and z. In particular, as the norm of the modulus $\mathfrak{m}$ increases, the values of the RCFPs get further from the origin (the points "go off to infinity"). This problem did not exist in the Gaussian period setting since all roots of unity lie on the unit circle, and so they were bounded in size. Because of this issue, we would like to rescale the RCFPs in some "nice" way so that the RCFP plots are contained within some bounded region.



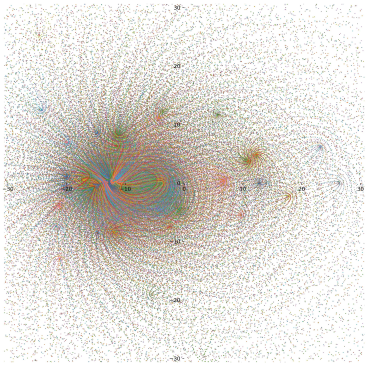
(a) $D = 1$, $m = 1155$, $A = 631$, $d = 5$



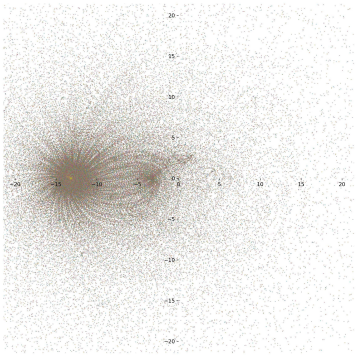
(b) $D = 3$, $m = 1265$, $A = 759 + 254\alpha$, $d = 3$



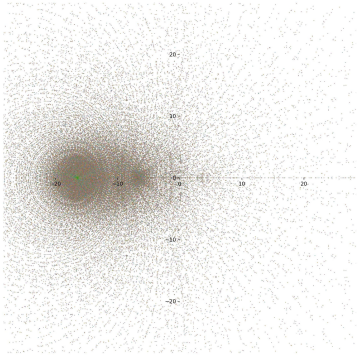
(c) $D = 7$, $m = 1265$, $A = 1 + 253\alpha$, $d = 3$



(d) $D = 19$, $m = 1155$, $A = 1079 + 1078\alpha$, $d = 4$



(e) $D = 67$, $m = 1099$, $A = 713 + 1085\alpha$, $d = 4$



(f) $D = 163$, $m = 1273$, $A = 135 + 1206\alpha$, $d = 5$

Figure 4.3. RCFP plots for the element A and modulus (m), where $K = \mathbb{Q}(\sqrt{-D})$

One natural idea is to map RCFPs to the unit disc so that the images are all uniform in size, and the "nice" property of our mapping is for it to be conformal. Unfortunately, there are no conformal mappings from $\mathbb{C}$ to the unit disc, so we decided to make do with a rescaling of points that was less nice. We note that we lack knowledge in this area, however, so there could very well be a rescaling map that handles this issue better than the one we describe below.

If $w \in \text{img}(\eta_{K,\mathfrak{m},A})$, we rescale using the map

$$w \mapsto \frac{w}{|w| + \sqrt[4]{|\text{Nm}(\mathfrak{m})|}},$$

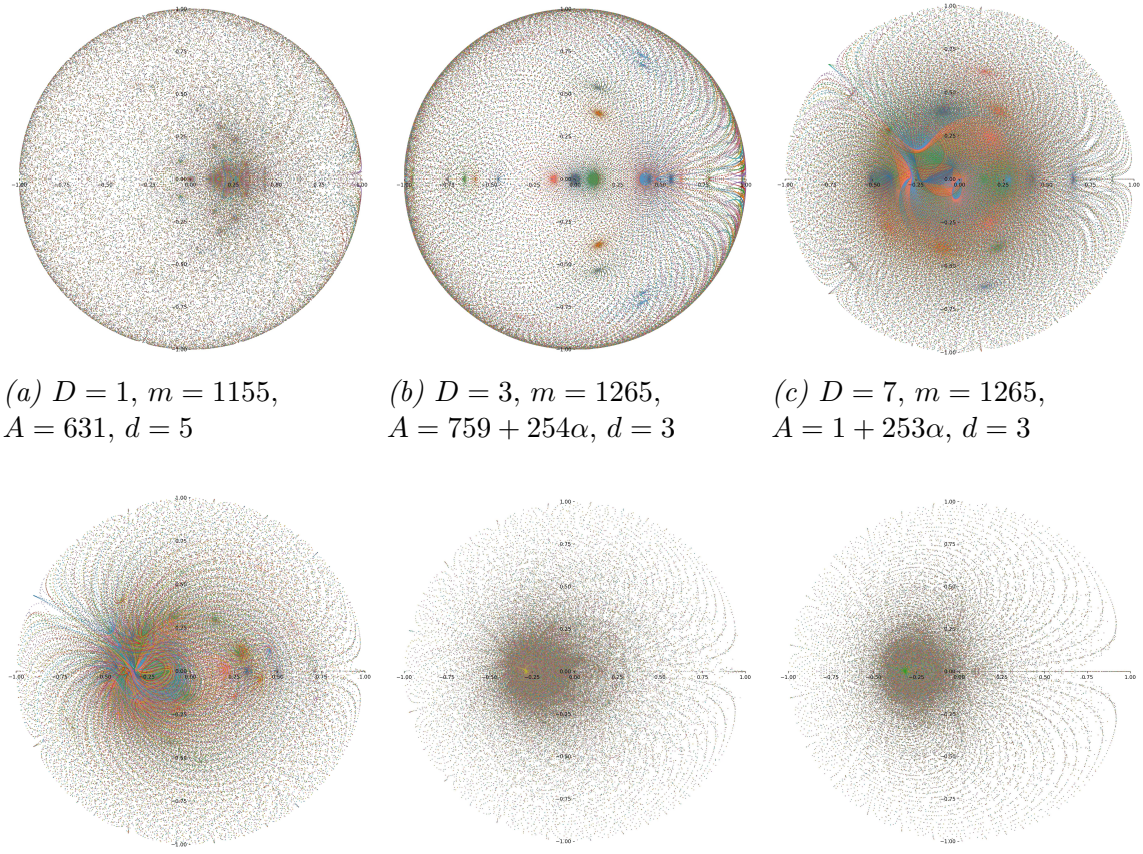
where Nm is the norm map from K to $\mathbb{Q}$. In the case where $\mathfrak{m} = (m)$, this map reduces to $w \mapsto \frac{w}{|w| + \sqrt{m}}$. Additionally, we note that the choice of using the 4th root was an ad hoc choice that seemed to generate images whose patterns were the easiest to see (at least for the cases where $D \neq 1, 3$), since the points were close enough together to see patterns while also not being so close that everything blurred together. We provide some examples of RCFP plots using this rescaling in Figure 4.4.

4.4 Observations

There are many observations that can be made about these RCFP plots, though these patterns seem difficult to explain for reasons that will be discussed in the next section.

We begin by exploring what happens in the analogous situation to the DGL Theorem and its generalization, Theorem 3.4. We choose a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$ and a modulus $m = p^e$, where p is a rational prime and e is some power. We choose an element A of the Galois group such that the multiplicative order d of A mod p^e divides $\#(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)$, where $\mathfrak{p} \subseteq \mathcal{O}_K$ is the prime lying over p. That is, the order d divides the size of the residue field of $\mathfrak{p}$, so $d \mid (p^2 - 1)$ when p is inert or $d \mid (p - 1)$ when p is split or ramified.

We then want to determine the behavior of these RCFP plots as d is fixed, but the size of m increases. We provide examples of this situation in Figure 4.5. Note that for these examples, we use the field $K = \mathbb{Q}(\sqrt{-7})$ and we fix the order of A to be 3.



(a) $D = 1$, $m = 1155$, $A = 631$, $d = 5$

(b) $D = 3$, $m = 1265$, $A = 759 + 254\alpha$, $d = 3$

(c) $D = 7$, $m = 1265$, $A = 1 + 253\alpha$, $d = 3$

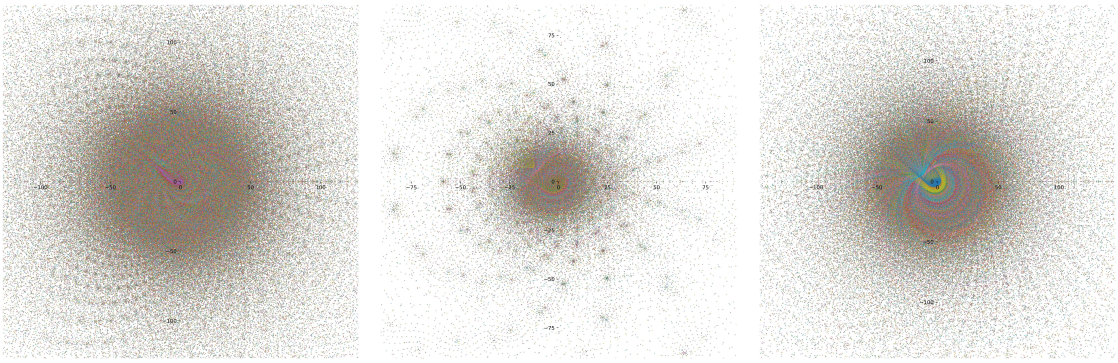
(d) $D = 19$, $m = 1155$, $A = 1079 + 1078\alpha$, $d = 4$

(e) $D = 67$, $m = 1099$, $A = 713 + 1085\alpha$, $d = 4$

(f) $D = 163$, $m = 1273$, $A = 135 + 1206\alpha$, $d = 5$

Figure 4.4. RCFP plots which have been rescaled to the unit disc, using the element A and the modulus (m), where $K = \mathbb{Q}(\sqrt{-D})$

Note that there appear to be certain areas where points seem to accumulate more densely, and this pattern seems to be more pronounced in the case when p is inert (Figure 4.5a) or split (Figure 4.5b) compared to the ramified case (Figure 4.5c). Additionally, these accumulation areas appear to show up at regular intervals, though the number of such areas doesn't seem to have any obvious correlation to the primes in the modulus. This last point provides evidence for the provability of some analogue of the DGL Theorem. That is, it would be expected that the ac-



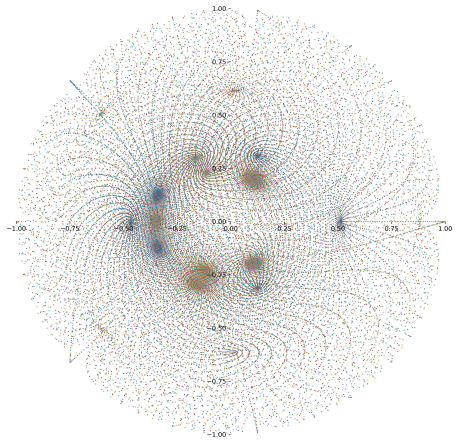
(a) $m = 5^4$, $A = 211 + 423\alpha$ *(b)* $m = 919$, $A = 52$ *(c)* $m = 7^4$, $A = 1353$

Figure 4.5. RCFP plots for $D = 7$, modulus (m), and A of order $d = 3$

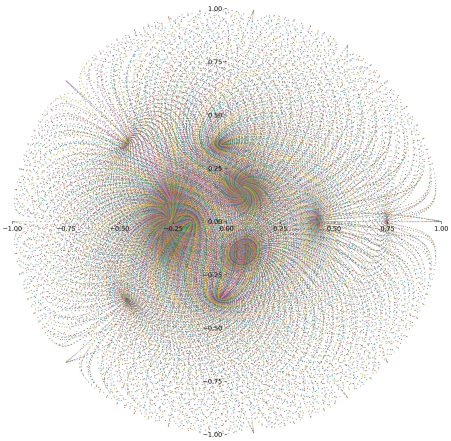
cumulation points are unrelated to the modulus in this case (recall that the most important property in the DGL Theorem was the order of ω modulo n, not the modulus itself).

For the next situation, we again choose a modulus $m = p^e$, but instead of choosing A such that d doesn't divide p, we choose A so that $d = p^b$ for some $b < e$. Note that in the Gaussian period setting, this situation leads to a Gaussian period plot that is a circle of radius p^b, along with a point at the origin. The situation for RCFP plots is a bit more interesting. We provide examples of this in Figure 4.6, where we again use the field $K = \mathbb{Q}(\sqrt{-7})$. Also, note that we used the map mentioned at the end of Section 4.3, since the patterns become more visible under this rescaling.

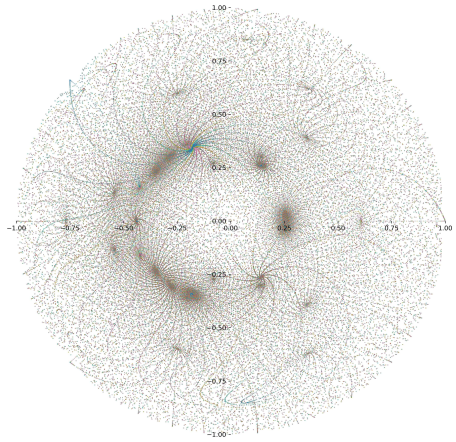
The images in this situation are rather striking, as they tend to have easily identifiable lines. In fact, similar to the images in Figure 4.5, there again seem to be areas where points seem to accumulate more densely; however, in this situation, these accumulation areas often have much more obvious spiral-like patterns appearing. We've taken to calling these areas "galaxies."



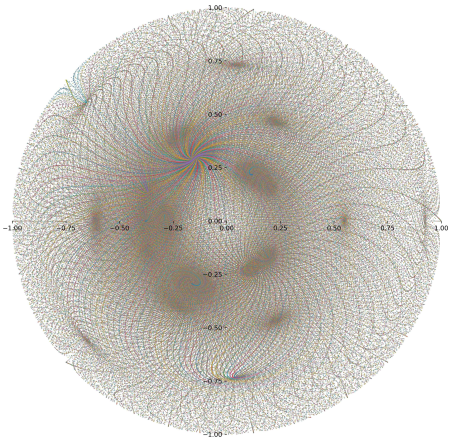
(a) $m = 5^4$, $A = 126 + 125\alpha$



(b) $m = 3^6$, $A = 1 + 343\alpha$



(c) $m = 11^3$, $A = 1 + 121\alpha$



(d) $m = 7^4$, $A = 1 + 343\alpha$

Figure 4.6. RCFP plots for $D = 7$, modulus (m) for $m = p^a$, and A of order $d = p$

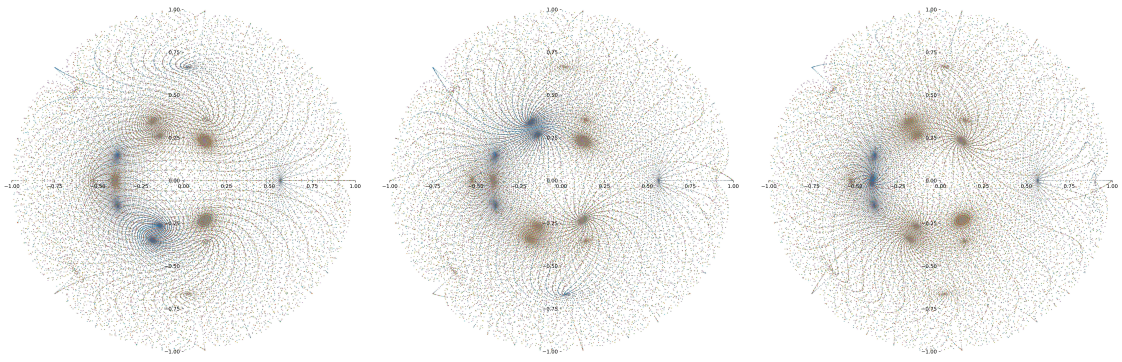
Another observation to make is that—unlike the analogous situation of the DGL Theorem in Figure 4.5—there does seem to be a correlation between the number of these galaxies and the primes in the modulus. For example, one notes that when $m = 5^4$ in Figure 4.6a, one can make out five red, green, and purple galaxies close to the origin, as well as five primarily blue galaxies which are further out. This pattern seems to continue further away from the origin, though it's difficult

to make out the finer details. Figure 4.6b provides another example of this phenomenon when $m = 3^6$, where there are three primarily blue, red, and green galaxies close to the origin.

Another notable feature here is that if A and B are two elements of the Galois group with the same multiplicative order p^b, then their respective RCFP plots are not necessarily the same. This is different than the Gaussian periods case, where we have an identical Gaussian period plot for any $\omega \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ is p^b. This is because $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is cyclic, while $(\mathcal{O}_K/p^e\mathcal{O}_K)^\times$ is not cyclic when p splits or when $e > 1$. In fact, we have the following isomorphism of abelian groups:

$$(\mathcal{O}_K/p^e\mathcal{O}_K)^\times \cong \begin{cases} \mathbb{F}_{p^2}^\times \times (\mathbb{Z}/p^{e-1}\mathbb{Z} \times \mathbb{Z}/p^{e-1}\mathbb{Z}) & p \text{ is inert,} \\ (\mathbb{Z}/p^e\mathbb{Z})^\times \times (\mathbb{Z}/p^e\mathbb{Z})^\times & p \text{ splits,} \\ \mathbb{F}_p^\times \times (\mathbb{Z}/p^e\mathbb{Z} \times \mathbb{Z}/p^{e-1}\mathbb{Z}) & p \text{ is ramified.} \end{cases}$$

In Figure 4.7, we provide examples of three distinct RCFP plots, even though the field $K = \mathbb{Q}(\sqrt{-7})$, the modulus $m = 5^4$, and the order $d = 5$ are fixed in all three cases.



(a) $m = 5^4$, $A = 376 + 250\alpha$ *(b)* $m = 5^4$, $A = 1 + 125\alpha$ *(c)* $m = 5^4$, $A = 501 + 250\alpha$

Figure 4.7. RCFP plots for $D = 7$, modulus (m) for $m = 5^4$, and A of order $d = 5$

Note in particular that the differences between these plots are more substantial than a simple change of coloring. For example, note the behavior of the points along the positive real axis. In Figure 4.7a, the string of points stays entirely on the real axis, while in Figures 4.7b and 4.7c, the string of points veers off toward either the upper or lower half-plane respectively.

4.5 Obstacles

Thus far, we have yet to prove any properties of RCFP plots in the same rigorous mathematical way that we used with Gaussian periods. The reason for this is due almost entirely to the complexity of the Galois action on ray class fields of quadratic imaginary fields, whereas the Galois action on cyclotomic fields is much simpler. This section is dedicated to explaining this difference in complexity.

For the cyclotomic case, the action of the Galois group can be described concretely as a function on roots of unity. In particular, choose $\omega \in (\mathbb{Z}/n\mathbb{Z})^\times$, and consider its corresponding element $\sigma_\omega \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. The action of σ_ω on $\mathbb{Q}(\zeta_n)$ can be described as a function on roots of unity that maps $\zeta_n^a \mapsto \zeta_n^{\omega a}$. This function is easily described, and studying this map amounts to studying the arithmetic dynamics of the function $f_\omega(x) = x^\omega$, which is a simple enough task.

However, for the quadratic imaginary case, choose an element

$$A \in (\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times \Big/ \mathcal{O}_K^\times$$

and consider its corresponding element $\sigma_A \in \mathrm{Gal}(K[\mathfrak{m}]/K[1])$. Assume for this discussion that K is not $\mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$, and let x be the x-coordinate of an $\mathfrak{m}$-torsion point of an elliptic curve with CM by K. Then $x = \wp(z_x; \mathcal{O}_K)$ for some $z_x \in \mathbb{C}/\mathcal{O}_K$, where $\wp$ is the Weierstrass $\wp$-function. In Section 4.2, we described the action of A

on x to be

$$A \cdot x = \wp(Az_x; \mathcal{O}_K),$$

where the multiplication Az_x occurs in $\mathbb{C}/\mathcal{O}_K$. The question then arises whether or not we can describe this action in a "nice" way—i.e. where the arithmetic dynamics can be studied in a way similar to the Gaussian period case. Unfortunately, this appears to be much more complicated in the RCFP case, perhaps even prohibitively so.

Before looking at the RCFP case, we first introduce a relevant definition, proposition, and theorem.

Definition 4.25 (In VI.2 of [Sil86])**.** An elliptic function (relative to a lattice Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ such that

$$f(z + \lambda) = f(z)$$

for all $z \in \mathbb{C}$ and all $\lambda \in \Lambda$.

Proposition 4.26 (Theorem VI.3.1c of [Sil86])**.** *The Weierstrass $\wp$-function $\wp(z; \Lambda)$ is an even elliptic function relative to Λ.*

Theorem 4.27 (Theorem VI.3.2 of [Sil86])**.** *Every even elliptic function relative to Λ is a rational function in $\wp(z; \Lambda)$.*

Now, for $A \in (\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times \,/\, \mathcal{O}_K^\times$, we define the function $f_A : h(E) \to h(E)$ so that f_A describes the Galois action of A. In particular, the function f_A comes from the following composition of maps:

$$\begin{array}{ccc} h(E) & \xrightarrow{f_A} & h(E) \\ {\scriptstyle x \mapsto z_x}\downarrow & & \uparrow{\scriptstyle z \mapsto \wp(z;\mathcal{O}_K)} \\ \mathbb{C}/\mathcal{O}_K & \xrightarrow{z \mapsto Az} & \mathbb{C}/\mathcal{O}_K \end{array}$$

Thus $f_A(x) = A \cdot x$. In the next paragraph, we show that the composition of the second and third maps above (which sends $z \mapsto \wp(Az; \mathcal{O}_K)$) is an even elliptic function relative to $\mathcal{O}_K$. By a slight abuse of terminology, we will then extend these properties to say that f_A is an even elliptic function. The reason for adding the map $x \mapsto z_x$ is to allow us to compose f_A with itself, which will be necessary to discuss RCFPs.

Now, first note that $z \mapsto \wp(Az; \mathcal{O}_K)$ is an even function, which comes directly from the fact that $\wp$ is an even function. Additionally, if $\lambda \in \mathcal{O}_K$, then $A\lambda \in \mathcal{O}_K$ (because $\lambda \in \mathcal{O}_K$ and $A \in (\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times/\mathcal{O}_K^\times$). Thus we have the following:

$$\wp(A(z+\lambda); \mathcal{O}_K) = \wp(Az + A\lambda; \mathcal{O}_K) = \wp(Az; \mathcal{O}_K),$$

where the second equality comes from the fact that $A\lambda \in \mathcal{O}_K$ and that $\wp(z; \mathcal{O}_K)$ is elliptic relative to $\mathcal{O}_K$. Thus the map $z \mapsto \wp(Az; \mathcal{O}_K)$ is also an elliptic function relative to $\mathcal{O}_K$, and so f_A is an even elliptic function relative to $\mathcal{O}_K$ (using the abuse of terminology mentioned above). Thus by Theorem 4.27, the function $f_A(x)$ is actually rational in $x := \wp(z_x; \mathcal{O}_K)$.

Now, recall that RCFPs are defined as

$$\eta_{K,\mathfrak{m},A} : \mathcal{O}_K/\mathfrak{m}\mathcal{O}_K \to \mathbb{C}, \qquad \eta_{K,\mathfrak{m},A}(z_x) = \sum_{j=0}^{r-1} \wp(A^j z_x; \mathcal{O}_K),$$

and note that

$$\wp(A^j z_x; \mathcal{O}_K) = (\underbrace{f_A \circ \cdots \circ f_A}_{j \text{ times}})(x).$$

Let us write $f_A^{(j)}(x)$ to represent this j-fold self-composition. Then we can rewrite RCFPs in the following way:

$$\eta_{K,\mathfrak{m},A} : h(E[\mathfrak{m}]) \to \mathbb{C}, \qquad \eta_{K,\mathfrak{m},A}(x) = \sum_{j=0}^{r-1} f_A^{(j)}(x).$$

Thus the study of RCFP plots is the study of the arithmetic dynamics of the rational functions f_A.

Now, studying the arithmetic dynamics of f_A requires computing $f_A(x)$ explicitly as a rational function. If A is an integer, then $f_A(x)$ can be built from the standard division polynomials for the elliptic curve isomorphic to $\mathbb{C}/\mathcal{O}_K$ (i.e. polynomials whose roots are the A-torsion points). These are defined recursively and depend on the choice of base field, but they are relatively well-known (see [Sil86, Exercise III.3.7]). For general $A \in (\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times$, however, computing f_A becomes more difficult, since this requires computing the generalized division polynomials, which are much more complex.

That being said, algorithms do exist for computing these polynomials. To the author's knowledge, Satoh in 2004 in [Sat04] was the first to describe such an algorithm, followed by an optimization of Küçüksakallı in 2015 in [KÏ5].

Regardless, these division polynomials remain difficult to describe without simply computing them explicitly. Additionally, even if one computes the generalized division polynomial ψ_A for some $A \in (\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times$, the complexity of ψ_A grows with $|\mathrm{Nm}(A)|$. In particular, both the degree and the number of nonzero terms of ψ_A increase with the size of A. Studying the arithmetic dynamics of polynomials becomes increasingly difficult as the number of nonzero terms increases, and since f_A is a actually a *rational* function depending on ψ_A, then studying the arithmetic dynamics of f_A becomes even more difficult.

However, we believe that studying RCFPs to be worthwhile mathematically, and we hope that this discussion might spark some interest in studying the rational functions f_A more explicitly.

APPENDIX

CODE

Most of the code used to generate these images was written in Python, though Sage was also used for convenience reasons to generate the animations (explained in Section 2.2) and the Laurent polynomials g_d (explained in Theorem 1.2 and Section 2.1). Many algorithmic aspects of computing elliptic curve torsion points were based on the algorithms in [CS08, Coh93], and these are often cited in the comments of the code itself. Readers may access our code at the following GitHub link:

https://github.com/SamanthaPlatt/GaussianPeriodsandAnaloguesCode

BIBLIOGRAPHY

[AAB+12] Marcelo Aguiar, Carlos André, Carolina Benedetti, Nantel Bergeron, Zhi Chen, Persi Diaconis, Anders Hendrickson, Samuel Hsiao, I. Martin Isaacs, Andrea Jedwab, Kenneth Johnson, Gizem Karaali, Aaron Lauve, Tung Le, Stephen Lewis, Huilan Li, Kay Magaard, Eric Marberg, Jean-Christophe Novelli, Amy Pang, Franco Saliola, Lenny Tevlin, Jean-Yves Thibon, Nathaniel Thiem, Vidya Venkateswaran, C. Ryan Vinroot, Ning Yan, and Mike Zabrocki. Supercharacters, symmetric functions in noncommuting variables, and related hopf algebras. *Advances in Mathematics*, 229(4):2310–2337, March 2012.

[ACDS04] Ery Arias-Castro, Persi Diaconis, and Richard Stanley. A super-class walk on upper-triangular matrices. *Journal of Algebra*, 278(2):739–765, 2004.

[AL21] Carlos A.M. André and Jocelyn Lochon. Supercharacters of discrete algebra groups. *Forum Mathematicum*, 35:221–244, 2021.

[And95] Carlos A.M. André. Basic characters of the unitriangular group. *Journal of Algebra*, 175(1):287–319, 1995.

[And01] Carlos A.M. André. The basic character table of the unitriangular group. *Journal of Algebra*, 241(1):437–471, 2001.

[BBF+14] J. L. Brumbaugh, Madeleine Bulkow, Patrick S. Fleming, Luis Alberto Garcia German, Stephan Ramon Garcia, Gizem Karaali, Matt Michal, Andrew P. Turner, and Hong Suh. Supercharacters, exponential sums, and the uncertainty principle. *J. Number Theory*, 144:151–175, 2014.

[BBGG+13] 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. *Exp. Math.*, 22(4):421–442, 2013.

[Chi09] Nancy Childress. *Class field theory*. Universitext. Springer, New York, 2009.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Cox13] D.A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2013.

[CS08] Henri Cohen and Peter Stevenhagen. Computational class field theory. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 497–534. Cambridge Univ. Press, Cambridge, 2008.

[DGL15] William Duke, Stephan Ramon Garcia, and Bob Lutz. The graphic nature of Gaussian periods. *Proc. Amer. Math. Soc.*, 143(5):1849–1863, 2015.

[DI08] Persi Diaconis and I. M. Isaacs. Supercharacters and superclasses for algebra groups. *Trans. Amer. Math. Soc.*, 360(5):2359–2392, 2008.

[DK23] Samit Dasgupta and Mahesh Kakde. Brumer-stark units and explicit class field theory. *Duke Mathematics*, 2023. (in press).

[DT09] Persi Diaconis and Nathaniel Thiem. Supercharacter formulas for pattern groups. *Trans. Amer. Math. Soc.*, 361(7):3501–3533, Jul 2009.

[EG20] Ellen Eischen and Stephan Garcia. A gallery of gaussian periods. In Carolyn Yackel, Robert Bosch, Eve Torrence, and Kristóf Fenyvesi, editors, *Proceedings of Bridges 2020: Mathematics, Art, Music, Architecture, Education, Culture*, pages 243–248, Phoenix, Arizona, 2020. Tessellations Publishing.

[FGK14] Christopher F. Fowler, Stephan Ramon Garcia, and Gizem Karaali. Ramanujan sums as supercharacters. *The Ramanujan Journal*, 35(2):205–241, Nov 2014.

[GHL15] Stephan Ramon Garcia, Trevor Hyde, and Bob Lutz. Gauss's hidden menagerie: from cyclotomy to supercharacters. *Notices Amer. Math. Soc.*, 62(8):878–888, 2015.

[HST22] Edmund Harriss, Katherine E. Stange, and Steve Trettel. Algebraic number starscapes. *Exp. Math.*, 31(4):1098–1149, 2022.

[KÏ5] Ömer Küçüksakallı. On the computation of generalized division polynomials. *Turkish J. Math.*, 39(4):547–555, 2015.

[Kat12] Nicholas M. Katz. *Convolution and Equidistribution*. Princeton University Press, Princeton, 2012.

[Kow13] Emmanuel Kowalski. Book reviews. https://www.ams.org/journals/bull/2014-51-01/S0273-0979-2013-01412-5/S0273-0979-2013-01412-5.pdf, 2013.

[KU23] Emmanuel Kowalski and Théo Untrau. Ultra-short sums of trace functions. *Mathematical Proceedings of the Cambridge Philosophical Society*, 210:367–390, 2023.

[Pla24] Samantha Platt. Visual aspects of gaussian periods and analogues. *International Journal of Number Theory*, 2024. (in press). References throughout are made to version 3 at https://arxiv.org/abs/2308.05220.

[Sat04] Takakazu Satoh. Generalized division polynomials. *Math. Scand.*, 94(2):161–184, 2004.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Thi10] Nathaniel Thiem. Branching rules in the ring of superclass functions of unipotent upper-triangular matrices. *Journal of Algebraic Combinatorics*, 31(2):267–298, Mar 2010.

[TV09] Nathanie Thiem and Vidya Venkateswaran. Restricting supercharacters of the finite group of unipotent uppertriangular matrices. *The Electronic Journal of Combinatorics*, 16(1), Feb 2009.

[Unt24] Théo Untrau. Equidistribution of exponential sums indexed by a subgroup of fixed cardinality. *Mathematical Proceedings of the Cambridge Philosophical Society*, 176(1):65–94, 2024.