Generating the Coefficient Field of Newforms with Inner Twists

Karen Ge

under the direction of

Robert Burklund
Department of Mathematics
Massachusetts Institute of Technology

January 17, 2019

Abstract

We investigate modular forms, which are 1-periodic functions on the complex upper half-plane that are related to elliptic curves. Since modular forms are periodic, they have a Fourier expansion. We consider the field E_f generated by adjoining the coefficients of this Fourier expansion to $\mathbb{Q}$. When this field has inner twists, a property of the automorphisms of E_f, we demonstrate an explicit connection between the probability of randomly generating the group of these twists and randomly generating the coefficient field E_f. Previous work focused on the probability that a single prime could generate the whole field; we extend these results by investigating the probability that n primes generate this field. We first relate previous results more directly to group theory by proving an explicit formula, then we show that this formula can be extended to choosing n primes and describe the group theoretic analogue.

1 Introduction

1.1 Motivation

Carl Friedrich Gauss once said that number theory is the queen of mathematics. Like any good sovereign, number theory hides many secrets. One of the most famous of these secrets is the modularity theorem, which was finally proven when Andrew Wiles finished the proof of Fermat's Last Theorem in 1995 [18]. His work sparked new developments in mathematics as well as greater public interest in meaningful mathematics [8]. The proof of this infamous theorem relied heavily on the study of elliptic curves and their relation to so-called Galois groups of number fields. The object that wraps up all these Galois groups into one is the absolute Galois group, denoted $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. This group has been hailed by many as the most mysterious object in mathematics ([16] p. 219). There are two broad approaches to studying this object. One is to look at its subgroups, which is equivalent to studying number fields. The other is to look at how $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ acts on vector spaces, the so-called Galois representations, which is where our work lies.

Wiles' proof solved part of another important, though younger, conjecture called the Langlands program. Proposed by Robert Langlands between 1967 and 1970, the Langlands program unifies many areas of mathematics with an ambitious series of conjectures [11]. In particular, it proposes hypotheses on the relationship between Galois representations, elliptic curves, and *modular forms*, a special class of complex functions. The $n = 1$ case of the Langlands program is equivalent to class field theory and was mostly resolved in the early half of the 20th century before Langlands connected those ideas to other areas. While significant progress has been made in the $n = 2$ case, several problems remain unresolved. Since the general case is still far out of reach, it would be fruitful to study the $n = 2$ case as completely as possible. Modular forms are particularly useful because they yield interesting yet tractable Galois representations.

1.2 Applications of modular forms

The study of modular forms not only connects Galois representations, elliptic curves, and algebraic geometry ([2], part 1), but it has also been applied to great effect in numerous other areas, including sphere-packing and string theory. Modular forms have been used to study the string theory realizations of elliptic curves [9]. More recently, Viazovska's seminal paper solving the sphere-packing problem for dimension 8 employed modular forms, and the same ideas also later solved the case of dimension 24, as shown in [17].

Modular forms are also intertwined with other areas of mathematics. They connect elliptic curves to other elliptic curves explicitly, and because of their numerous relations to Galois theory, they have been used to great effect in a number of seemingly disparate areas of mathematics, including class field theory, describing drums whose shape one cannot hear, Fermat's Last theorem, and cryptography (see [2] part 1).

Our work lies within the $n = 2$ case of the Langlands program. The resolution of the aforementioned modularity theorem allows us to prove statements about modular forms, where we have more control, and then use this connection to get corresponding statements about elliptic curves. We study newforms with inner twists and give an explicit formula that connects the generation of the coefficient field to the generation of certain subgroups. See Section 2.3 for definitions. These results build on the work of Koo, Stein, and Wiese [10] who proved results tying inner twists to the density of primes that generate the field of coefficients by itself. Their work shows that the set of such primes has density 1. However, in the case that the modular form f has inner twists, this density changes. We investigate the case when f has inner twist and extend their result by giving a formula for the probability that n coefficients generate this field.

In Section 2, we define fundamental ideas and the relevant background. In Section 3 we elaborate on the work of Koo, Stein, and Wiese in order to state our problem precisely, and in Section 4 we prove our main theorem. Our theorem shows that the probability of generating a newform with inner twists is the same as the probability of generating the full group of its inner twists.

Finally, we offer some suggestions for future work in Section 5.

2 Background and Definitions

We first define important concepts and notation, starting with modular forms, the Hecke operators that act on them, their level structure, newforms, and inner twists. We omit some proofs that can be found in [15] or [6].

Definition 1. A *modular form* of weight $2k$ and nebentypus χ is a holomorphic function f on the complex upper half-plane $\mathcal{H}$ such that

- it is analytic on the upper half-plane
- it satisfies
$$f(z) = \chi(d)(cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) \qquad \text{for any } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}).$$

The matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ generate $SL_2(\mathbb{Z})$ (see [15], Chapter VII Theorem 2). Therefore, it suffices to check the modularity conditions for $f(Sz)$ and $f(Tz)$ in order to prove that f is modular.

Figure 3 shows a *fundamental domain* for the modular group $SL_2(\mathbb{Z})$.

A careful reader will question why the exponent in Definition 1 cannot be odd. Indeed, if we had an exponent of the form $2k+1$, then f must satisfy
$$f(z) = f\left(\frac{-z+0}{0-1}\right) = (0 \cdot z - 1)^{2k+1} f(z) = -f(z).$$
So $f \equiv 0$ and it is not a very interesting modular form.

As we saw above, modular forms are periodic with period 1. So they may be represented by a Fourier series, also called a q-expansion:
$$f(z) = \sum_{n=0}^{\infty} a_n(f) q^n,$$

where $q = e^{2\pi iz}$ and $a_n(f)$ denotes the n'th Fourier coefficient. We say a modular form is *cuspidal* if $a_0 = 0$.

2.1 Hecke operators

Now if we consider the space of modular forms, a natural question is that of what operators can act on the space. A canonical example is the Hecke operators.

Definition 2. The mth *Hecke operator* is a linear operator T_m that acts on the vector space modular forms of weight k. We have

$$T_m f(z) = m^{k-1} \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1 \backslash \mathcal{M}_m} (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right), \tag{1}$$

where $\mathcal{M}_m$ is the set of 2×2 integral matrices of determinant m and Γ_1 is $SL_2(\mathbb{Z})$.

The Hecke operators are only well-defined when f is modular ([2], Part 1 Section 4).

When the modular form is cuspidal, we have $a_0 = 0$, so we find that the nth coefficient of $T_m f = \sum_{n=1}^{\infty} b_n q^n$ is

$$b_n = \sum_{\substack{r \mid (m,n), \\ r>0}} r^{k-1} a_{mn/r^2}, \tag{2}$$

where the a_i are the coefficients of f and (m, n) denotes $\gcd(m, n)$ (see [2], Part 1 Chapter 1 for details). Furthermore, Eq. (2) also shows that the Hecke operators are commutative, i.e. $T_m T_n f = T_n T_m f$. It is for this reason that we are able to simultaneously diagonalize the operators to get a basis, which is explained further in Section 2.3.

Definition 3. A modular form f of weight k is called an *eigenform* for a Hecke operator T_m if it satisfies $T_m f = \lambda_m f$ for some eigenvalue of λ_m.

The modular form f is called a *simultaneous eigenform* for multiple Hecke operators if it is an eigenform for each of them.

Next we show that, when studying the field generated by the Fourier coefficients of cuspidal eigenforms, we need only look at the prime-indexed coefficients. In other words,

$$\mathbb{Q}\big(a_p(f) \mid p \text{ prime}\big) = \mathbb{Q}\big(a_n(f)\ \forall\, n\big).$$

First, we normalize the modular form by dividing all coefficients by a_1, so that the coefficient of q becomes 1. Then the q-expansion of f starts with $q + \ldots$ and the q-expansion of $T_m f$ starts with $b_1 = 1^{k-1} a_{1 \cdot m} = a_m q$ by Eq. (2). Thus the eigenvalue λ_m must be a_m for such modular forms. Applying the equation $T_m f = a_m f$ and looking at the coefficient a_n of f, we find

$$a_m a_n = \sum_{r|(m,n)} r^{k-1} a_{mn/r^2},$$

so in particular, if $(m, n) = 1$, we see that $a_{mn} = a_m a_n$. Furthermore, a_{p^b} is directly related to a_{p^c} for $c < b$ as well, so when considering adjoining the coefficients to $\mathbb{Q}$, it suffices to consider only the prime-indexed coefficients.

It is important to note that since the eigenvalues must be algebraic [14], the a_m must also be algebraic. Thus the field generated by the Fourier coefficients is a number field.

2.2 Level Structure

Here we set up the notion of newforms by considering the level structure of modular forms. For $N \in \mathbb{N}$, we first define $\Gamma_0(N)$, a congruence subgroup of $SL_2(\mathbb{Z})$:

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \mid c \equiv 0 \pmod{N},\ ad - bc = 1 \right\}.$$

We consider functions f that satisfy the conditions of Definition 1 but with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)$ from the subgroup $\Gamma_0(N)$ of $SL_2(\mathbb{Z})$. We say that these modular forms have *level* N. The space of modular forms of level N is larger than the space of modular forms associated to $SL_2(\mathbb{Z})$, and the the space for level MN is larger than the space for level N. The theory of Hecke operators can be extended to this level structure by replacing the Γ_1 in Eq. (1) with $\Gamma_0(N)$.

2.3 Newforms

Let $\mathcal{M}_k(\Gamma_0(N))$ be the space of modular forms of weight k and level N, and let $\mathcal{S}_k(\Gamma_0(N))$ be the corresponding space of cuspidal forms. To focus on set of eigenforms that form a basis for $\mathcal{M}_k$, we use the Petersson inner product to get an inner product space of modular forms.

We then split the space of eigenforms of level N into those that are produced from levels $N' \mid N$ and *newforms* that first appear at level N. Note that newforms of level N continue to appear at higher levels, just not at lower ones. More concretely, we have the inclusion diagram Figure 1.

$$\begin{tikzcd}
\mathcal{M}_k(\Gamma_0(N)) \arrow[r, phantom, "\supseteq"] & \mathcal{S}_k(\Gamma_0(N)) \arrow[r, phantom, "\supseteq"] \arrow[d, phantom, "\cup|"] & \mathcal{S}_k(\Gamma_0(N))^{\text{new}} \\
 & \mathcal{S}_k(\Gamma_0(N))^{\text{old}} &
\end{tikzcd}$$

Figure 1: Breaking up $\mathcal{S}_k(\Gamma_0(N))$ into the set of newforms $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ and the set of oldforms $\mathcal{S}_k(\Gamma_0(N))^{\text{old}}$

When we diagonalize the Hecke operators, we find that the oldforms are the orthogonal complement of the newforms under the Petersson inner product on this space of cusp forms (more details in [6], Section 5.6).

Definition 4. A *newform* of level N and weight k is a cuspidal modular form $f \in \mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ that is normalized so that $a_1(f) = 1$.

For the remainder of this paper, we focus on newforms.

2.4 Twists and Inner Twists

We define the coefficient fields we will be studying:

$$E_f = \mathbb{Q}\Big(a_n(f) \mid (n, N) = 1\Big), \tag{3}$$

$$F_f = \mathbb{Q}\left(\frac{a_n(f)^2}{\chi(n)} \mid (n, N) = 1\right) \tag{4}$$

for each modular form f with nebentypus χ.

Key to our investigation is an operator on modular forms called *twisting*. A Dirichlet character ϵ called a twist can act on f as described below.

Definition 5. A *Dirichlet character* ϵ is a map from $\mathbb{Z}$ to $\mathbb{C}$ such that

- There is some N such that $\epsilon(a+N)=\epsilon(a)$ for all integers a,
- $\epsilon(n)=0$ if and only if $\gcd(n,N)\neq 1$, and
- $\epsilon(m)\chi(n)=\epsilon(mn)$ for all $m,n\in\mathbb{Z}$.

To make sure N is minimal, we have the following notion.

Definition 6. The *conductor* of a Dirichlet character ϵ is the smallest positive integer N such that $\epsilon(a+N)=\epsilon(a)$ for all $a\in\mathbb{Z}$.

Definition 7. The *twist* of a modular form $f=\sum a_n q^n$ by ϵ is

$$f_\epsilon(z)=\sum a_n\epsilon(n)q^n. \tag{5}$$

A twist of a modular form is still modular. This follows from the fact proven in [13] that if f has nebentypus χ, then the nebentypus of its twist by ϵ is $\chi\cdot\epsilon^2$. Thus, with a few exceptions, when f has level N and ϵ has conductor M, the function f_ϵ will have level NM^2 (again, see [6] for details).

Following the definition in [10], we have the following.

Definition 8. A twist ϵ is *inner* if there exists a field automorphism $\sigma_\epsilon : E_f\to E_f$ such that

$$a_p(f)\epsilon(p)=\sigma_\epsilon(a_p(f)). \tag{6}$$

To illustrate the notion of inner twists, we analyze the following example, which is briefly considered in [10].

Example 1. Consider the modular form f of weight 2 and level 63 with the twist $\epsilon : p\mapsto\left(\frac{p}{3}\right)$, the Legendre symbol modulo 3, which sends squares (mod 3) to 1 and non-squares (mod 3) to -1.

From a brief calculation with SAGE, we find that the first few terms of the Fourier expansion for f are

$$f=q+\sqrt{3}\cdot q^2+q^4-2\sqrt{3}\cdot q^5+q^7-\sqrt{3}\cdot q^8-6q^{10}+2\sqrt{3}\cdot q^{11}+2q^{13}+\dots.$$

We see that the occurrences of $\sqrt{3}$ have two interesting properties. First, whenever it shows up as a coefficient it is always of the form $0 + c\sqrt{3}$ for $c \in \mathbb{Z}$. Second, it only shows up as a coefficient for q^a when $a \equiv 2 \pmod 3$.

The automorphism σ_ϵ associated to ϵ must satisfy Eq. (6), so for primes congruent to $2 \pmod 3$, we need $a_p(f)(-1) = \sigma_\epsilon(a_p(f))$. From our observations above, ϵ affects the signs of the $\sqrt{3}$'s, so it is natural to have σ_ϵ send $\sqrt{3}$ to $-\sqrt{3}$ and vice versa.

For the following result, we define Γ, the group of all the automorphisms σ_ϵ associated to the inner twists ϵ of f.

Lemma 2.1. *The field extension E_f of F_f is Galois.*

Proof. First we show that F_f is indeed a subfield of E_f. According to [10], the field E_f is either a field with complex multiplication or totally real. If it is totally real, the extension is necessarily Galois. Otherwise, the properties of the Petersson inner product on Hecke operators show that

$$\overline{a_p(f)} = \chi(p)^{-1} a_p(f),$$

and since every subfield of a field with complex multiplication is preserved by complex conjugation, we see that $\chi(p)^{-1}a_p(f)$ must be in F_f. Then $\mathbb{Q}(a_p(f)) \subseteq E_f$ must contain $\overline{a_p(f)}$, and so it contains $\chi_p^{-1}a_p(f)^2$ as well and $F_f \subseteq E_f$.

Now we see that F_f is the field fixed by the action of Γ on E_f because

$$\begin{aligned} \sigma_\epsilon\left(\frac{a_p(f)^2}{\chi(p)}\right) &= \sigma_\epsilon\big(a_p(f)\big)\sigma_\epsilon\left(\overline{a_p(f)}\right) \\ &= a_p(f)\epsilon(p)\overline{a_p(f)\epsilon(p)} \\ &= a_p(f)\overline{a_p(f)}, \end{aligned}$$

as desired. □

Note that Lemma 2.1 implies that there is a one-to-one correspondence between subgroups of Γ and intermediate fields L with $F_f \hookrightarrow L \hookrightarrow E_f$.

Finally, there is a group isomorphism between this Γ under composition and the group of the associated characters under multiplication, so from now on, we can consider Γ to be this group of associated characters.

3 From One to Many Coefficients

In this section we consider the structure of multiple coefficients $a_p(f)$. Our work builds on the following construction and result from [10].

Definition 9 (Koo, Stein, Wiese [10])**.** For a subgroup H of Γ consisting of the twists $\epsilon_1, \ldots \epsilon_r$, we define K_H to be the minimal number field on which all the ϵ_i are trivial, i.e., the field such that its absolute Galois group is the kernel of the map

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \xrightarrow{\epsilon_1,\ldots,\epsilon_r} \mathbb{C}^\times \times \cdots \times \mathbb{C}^\times.$$

Theorem 3.1 (Koo, Stein, Wiese [10])**.** *Define f, E_f, and F_f as in Eq.* (3) *and Eq.* (4)*. Let L be any subfield of E_f and let M_L be the set defined by*

$$\{p \text{ prime} \mid a_p(f) \in L\}.$$

Then if $F_f \subseteq L$, we have $L = E_f^H$, i.e. it is the subfield of E_f fixed by some subgroup $H \subseteq \Gamma$, and M_L has density

$$1/[K_H : \mathbb{Q}].$$

For convenience, we define $k_H = [K_H : \mathbb{Q}]$.

Note that when $H = \Gamma$ and f does not have any twists, then Γ is trivial, and the density of primes p such that $a_p(f)$ generates E_f is 1.

Theorem 3.1 gives a formula for the density of those primes p for which $a_p(f)$ generates E_f, but it is in terms of K_H, which *a priori* is not well-understood. We would like to make Definition 9 more explicit and find a formula for k_H. The following lemma (proof in Section 4) does so.

Lemma 3.2. *The density k_H equals $|H|$.*

Then we have enough information to ask about the probability that n random primes $p_1, \ldots p_n$ generate the field E_f. This question is important for fields E_f that cannot be generated by a single $a_p(f)$. We will show this occurs precisely when Γ is not cyclic. Indeed, consider the example below.

Example 2. Consider the newform f of level 512 and weight 2. Its group of inner twists, say $\{\mathbf{e}, \epsilon_1, \epsilon_2, \epsilon_3\}$, is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

This example is considered in [10], where Koo, Stein, and Wiese show that the density of the set of p such that $a_p(f)$ generates $E_f^{\langle \epsilon_1 \rangle}$, or the subfield of E_f fixed by ϵ_1, is $\frac{1}{4}$. The probability that one coefficient $a_p(f)$ generates E_f is 0, but if we consider choosing two coefficients, the probability is

$$1 - 3 \cdot \frac{1}{4} + 2 \cdot \frac{1}{4} \cdot \frac{1}{4} = \frac{3}{8}.$$

This example motivates us to ask the following.

Question 1. When is $\mathbb{Q}\big(a_{p_1}(f), a_{p_2}(f), \ldots, a_{p_n}(f)\big)$ equal to E_f? With what probability does this occur?

In order to answer this question, we use Lemma 3.2 to prove the following.

Theorem 3.3. *The probability* $\mathbb{P}\big(\mathbb{Q}(a_p(f)) = E_f^H\big)$ *is equal to the probability that a randomly chosen* $g \in \Gamma^\vee$ *has* $\ker(g) = H$*, where* $\Gamma^\vee$ *is the Pontryagin dual* $\mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z})$*.*

For convenience, we write $\mathbb{P}(= H)$ for the probability $\mathbb{P}\big(\mathbb{Q}(a_p(f)) = E_f^H\big)$.

Note that $\Gamma \cong \Gamma^\vee$ because Γ is a finite Abelian group (see Section 3 of [4]).

As an immediate corollary, since all finite subgroups of $\mathbb{Q}/\mathbb{Z}$ are cyclic, we have:

Corollary 3.3.1. $\mathbb{P}(= H)$ is positive if and only if its dual, $H^\vee$, is cyclic.

3.1 Concrete Illustrations

We consider inner twists $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ of conductor N. We can extend the map ϵ to get

$$\operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \operatorname{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\epsilon} \mathbb{C}^\times,$$

where $\operatorname{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ denotes the Galois group of the cyclotomic extension of $\mathbb{Q}$ with the primitive Nth roots of unity.

Essentially, instead of looking at the whole group $\operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ we restrict to adjoining the primitive Nth roots of unity ζ_N. That means that, since ϵ has period N, we can view the automorphisms as coming from $\operatorname{Hom}\big(\operatorname{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}), \mathbb{C}^\times\big)$. To illustrate this notion, we refer the reader to Appendix C. We provide an example about calculating probabilities from a subgroup structure.

Example 3. We consider the group $\Gamma = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. We find the probability of generating a specific subgroup from the probabilities k_H of generating a group $G \supseteq H$. Figure 2 depicts Γ pictorially with $\mathbf{e}$ as the trivial subgroup.

$$\begin{tikzcd}
A \arrow[r] & C \arrow[r] & \Gamma \\
\mathbf{e} \arrow[u] \arrow[r] & B \arrow[u] \arrow[r] & D \arrow[u]
\end{tikzcd}$$

Figure 2: The subgroup lattice of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$

Here the arrows represent inclusion of subgroups and the letters represent names of subgroups. We see that applying Theorem 3.1 only gives us the probabilities of being at a specific subgroup H or any of the groups that include it since a group that includes a specific H necessarily fixes the points that H fixes when acting on E_f. In fact, we have a poset structure on these subgroups, so writing inclusion as $<$ and the probability that the field generated by a coefficient is fixed by H as $\mathbb{P}(= H)$, etc., we find

- $\mathbb{P}(\geq \mathbf{e}) = 1$,

- $\mathbb{P}(> \mathbf{e}) = \mathbb{P}(\geq a) + \mathbb{P}(\geq b) - \mathbb{P}(\geq c)$,
- The probability of being $\geq H$ for any of the subgroups H is $1/k_H$

Therefore, $\mathbb{P}(= \mathbf{e}) = 1 - 1/k_a - 1/k_b + 1/k_c$. To connect back to the coefficient field, $\mathbb{P}(= \mathbf{e})$ is the probability that a single coefficient generates the subfield of E_f fixed by the identity, which is just E_f. So, in this particular case, we have an explicit formula for the probability that a single coefficient generates the entire coefficient field.

4 Connection to Statistics of Subgroups

Now we prove our general results on the density k_H. Given a group Γ of twists, let L be the least common multiple of their conductors.

Lemma 4.1. *Let H be the group of automorphisms $\sigma_{\epsilon_1}, \ldots, \sigma_{\epsilon_r}$ corresponding to inner twists $\epsilon_1, \ldots \epsilon_r$. Then k_H is equal to the size of the image of the map $\Psi : \mathbb{Z}/L\mathbb{Z} \to \mathbb{C}^\times \times \cdots \times \mathbb{C}^\times$ defined as the composite map of all the ϵ_i.*

Proof. Observe that K_H is the field of fixed points under $\ker(\Psi)$ of $\mathbb{Q}(\zeta_N)$, so it is necessarily a Galois extension. By the Fundamental Theorem of Galois theory, we have

$$[\mathbb{Q}(\zeta_N) : K_H] \cdot [K_H : \mathbb{Q}] = [\mathbb{Q}(\zeta_N) : \mathbb{Q}]. \tag{7}$$

In particular, because K_H is the fixed field, we see that

$$[\mathbb{Q}(\zeta_N) : K_H] = |\ker(\Psi)|.$$

But $|(\mathbb{Z}/N\mathbb{Z})^\times| = \varphi(N) = |\ker(\Psi)| \cdot |\text{im}(\Psi)|$, where φ denotes the Euler phi function. Combining Eq. (7) and the previous relation gives

$$k_H = [K_H : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_N) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_N) : K_H]} = \frac{\varphi(N)}{|\ker(\Psi)|} = |\text{im}(\Psi)|.$$

□

Now we prove that this image actually has size equal to $|H|$ by using homological algebra. We need the fact that $\mathbb{C}^\times$ is an injective $\mathbb{Z}$-module, which is fully explained and proven in Appendix B. The statement of the lemma follows.

Lemma 4.2. $\mathbb{C}^\times$ *is an injective* $\mathbb{Z}$*-module.*

As promised by Lemma 3.2, we can say more about $k_H = |\text{im}(\Psi)|$.

Proof of Lemma 3.2. We first observe that Ψ maps into $\mathbb{C}^\times \times \cdots \times \mathbb{C}^\times$, which is isomorphic to Functions$(H, \mathbb{C}^\times)$, the space of functions from H to $\mathbb{C}^\times$. Within that set, we have the homomorphism group $\text{Hom}(H, \mathbb{C}^\times)$, so we know that the image of Ψ is bounded by the size of that group, which is $|H|$. In symbols, $|\text{im}(\Psi)| \leq |H|$. We will show that the map into $\text{Hom}(H, \mathbb{C}^\times)$ is surjective, which will prove the other direction.

From Lemma 4.1 we know that k_H is equal to the size of the image of Ψ. As before, let L be the least common multiple of the conductors of the twists in H. The map Ψ is the composite map of generating characters in H.

For convenience let $A = (\mathbb{Z}/L\mathbb{Z})^\times$. Then from the universal property of tensor products, we know the map $A \to \text{Hom}(H, \mathbb{C}^\times)$ bijects to $A \otimes H \to \mathbb{C}^\times$, i.e. their homomorphism groups are isomorphic. We observe that if two elements x and y of H map to the same element of the group $\text{Hom}(A, \mathbb{C}^\times)$, then they must both act the same way on all coefficients of f and so $x = y$ since the twists themselves form a group. Thus, the map $H \hookrightarrow \text{Hom}(A, \mathbb{C}^\times)$ is injective. We will construct a short exact sequence to show that $A \to \text{Hom}(H, \mathbb{C}^\times)$ is surjective.

Define G such that $0 \to H \to \text{Hom}(A, \mathbb{C}^\times) \to G \to 0$ is a short exact sequence. Then we have the short exact sequence

$$0 \to \text{Hom}(G, \mathbb{C}^\times) \to \text{Hom}\big(\text{Hom}(A, \mathbb{C}^\times), \mathbb{C}^\times\big) \to \text{Hom}(H, \mathbb{C}^\times) \to 0.$$

It is injective on the left because of the properties of the homomorphism group. We have surjectivity on the right by the injectivity of $\mathbb{C}$, in particular, condition (2) of Definition 10.

But $\text{Hom}\big(\text{Hom}(A, \mathbb{C}^\times), \mathbb{C}^\times\big) \cong A$ where the isomorphism is the evaluation map that sends $a \in A$ to the function $f \mapsto f(a)$. Thus we have the surjectivity of $A \twoheadrightarrow \text{Hom}(H, \mathbb{C}^\times)$. Then everything in $\text{Hom}(H, \mathbb{C}^\times)$ has a preimage in A, which means that all possible outputs are mapped to, and in particular, $|\text{im}(\Psi)| = |H|$. □

So far, we have shown that the probability of a single prime generating a field containing some E_f^H is $1/|H|$ by combining Theorem 3.1, Lemma 4.1, and Lemma 3.2. To extend this idea to n primes, we must show that generating a field with some $a_p(f)$'s has the same statistics as a random element of $\Gamma^\vee$ generating a subgroup $H^\vee$. We illustrate this idea with the example below.

Example 4. Take $\Gamma = C_9 \times C_3$. The poset of its subgroups is shown in Figure 4.

We have two different types of C_3 subgroups in Γ. The first, which we call $C_3(a)$, is the intersection of all the subgroups of order 9. So if we represent elements of Γ as ordered pairs (a, b) for $a \in \mathbb{Z}/9\mathbb{Z}$ and $b \in \mathbb{Z}/3\mathbb{Z}$, then $C_3(a) = \{(0,0),(3,0),(6,0)\}$. The other three subgroups of order 3 are generated by $(3,1)$, $(3,2)$, and $(0,1)$.

Applying Lemma 3.2 and the ideas of Example 3, we obtain Table 1.

Now, how does the duality come into play? We observe that both $(3,0)$ and $(6,0)$ generate the subgroup we named $C_3(a)$. The cokernel of the dual of $C_3(a)$ is $(C_9 \times C_3)/C_3(a)$, which is isomorphic to $C_3 \times C_3$. So there is a $\frac{2}{27}$ chance that picking a random element of $C_3 \times C_9$ has a cokernel with its dual equal to $C_3 \times C_3$. The probability that choosing some $a_p(f)$ generates the field of E_f fixed by $C_3 \times C_3$ is also $\frac{2}{27}$. We now formalize these observations.

Proof of Theorem 3.3. From Lemma 3.2, we know that the density of primes p for which $a_p(f)$ generates a field that extends some E_f^H is exactly $1/|H|$. To generalize the reasoning of Example 3, we apply the principle of inclusion-exclusion:

$$\mathbb{P}(=H) = \mathbb{P}(\geq H) - \sum_{G,\ G \supseteq H} \mathbb{P}(=G).$$

Furthermore, the probability that some element g generates $H^\vee$, the dual of H, is

$$\mathbb{P}\left(\langle g \rangle = H^\vee\right) = \mathbb{P}\left(\langle g \rangle \leq H^\vee\right) - \sum_{K, K \subseteq H^\vee} \mathbb{P}\left(\langle g \rangle = K^\vee\right).$$

By Theorem 3.11 of [4], the lattice of the poset of subgroups is preserved under the Pontryagin duality, so for each $G \supseteq H$ in the formula for $\mathbb{P}(=H)$, its dual $G^\vee$ is included in $H^\vee$. So it suffices to check that the probability that $\langle g \rangle = G$ for some $G \supseteq H^\vee$ is the same as the probability that $a_p(f)$ generates E_f^H.

But $\mathbb{P}(\langle g\rangle = G)$, $G \supseteq H^\vee$ is exactly the probability that g is an element of $H^\vee$, which is exactly $1/|H|$. Thus, $\mathbb{P}(=H) = \mathbb{P}(\langle g\rangle = H^\vee)$. □

If we decompose Γ into its p-components as in the proof of Lemma 3.2, we can bound the number of coefficients needed to generate all of E_f. Suppose that each Γ_{p_i} is a product of r_i cyclic summands. Then we have the following corollary.

Corollary 4.2.1. We need at most $\max_i(r_i)$ coefficients to generate all of E_f.

Sketch of proof. To generate Γ we need a set of elements of the form $(g_1, g_2, \ldots, g_n)$. We can use the Chinese Remainder Theorem to create elements that generate as many of the H_{p_i} as possible at once. The maximum number of such elements we need is equal to the maximum number of summands, each of which has its own generator, that some H_{p_i} has. □

5 Conclusion and Future Work

We reduced the problem of generating the coefficient field of a modular form to the statistics of subgroups, which is a well-studied, though not completely-solved problem [3]. We were able to generalize the results of Koo, Stein, and Wiese by making them more explicit, thus allowing us to investigate generating a coefficient field with n prime-indexed coefficients. In particular, we have the theorem below. The method of proof is essentially to check that the lattice structure is preserved, i.e. that intersection and union for fields translate correctly to the group theory side. We are still working on the details.

Theorem 5.1. *The probability* $\mathbb{P}\big(\mathbb{Q}(a_{p_1}(f), \ldots, a_{p_n}(f)) = E_f^H\big)$ *is equal to the probability that a n randomly chosen elements* $g_1, g_2, \ldots g_n \in \Gamma^\vee$ *has* $\ker(\times_i g_i) = H$*, where* $\Gamma^\vee$ *is the Pontryagin dual* $\mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z})$*.*

One interesting question that arose when experimenting with examples is the following.

Question 2. Given a finite Abelian group Γ, is always possible to construct a newform f such that its group of inner twists is isomorphic to Γ?

In the future, we hope to consider the implications of this result for elliptic curves and for the Galois representations of modular forms with inner twists. Perhaps future work can continue to investigate the role inner twists play in Galois theory and in the various applications of modular forms or for modular forms with complex multiplication.

6 Acknowledgments

I would first like to thank my mentor Robert Burklund. He provided invaluable guidance throughout the entire process. Dr. John Rickert, my academic tutor, taught me many things about giving presentations and writing papers, for which I am very thankful. I am also very grateful to Dr. Tanya Khovanova for her support and guidance as well as Professors Ankur Moitra and Davesh Maulik from the MIT Math Department for organizing the mathematics mentorships. I would also like to thank MIT, CEE, and RSI for giving me the very humbling opportunity to attend the Research Science Institute.

I would also like to thank Ankur Moitra and Miles Edwards for their mathematical comments, Blythe Davis, Svetlana Markarova, and David Wu for their many suggestions, and my parents Kejia Ho and Yi Ge for their unfailing support. Finally, I would like to recognize the sponsors of MIT, CEE, and RSI, as well express my gratitude to my personal sponsors, Ms. Andrea Ricci, Ms. Margo Leonetti O'Connell, Mr. Nicholas S. Gouletas, Mr. Wendell Maddox, and Dr. Jason Koh.

A Figures and Exposition

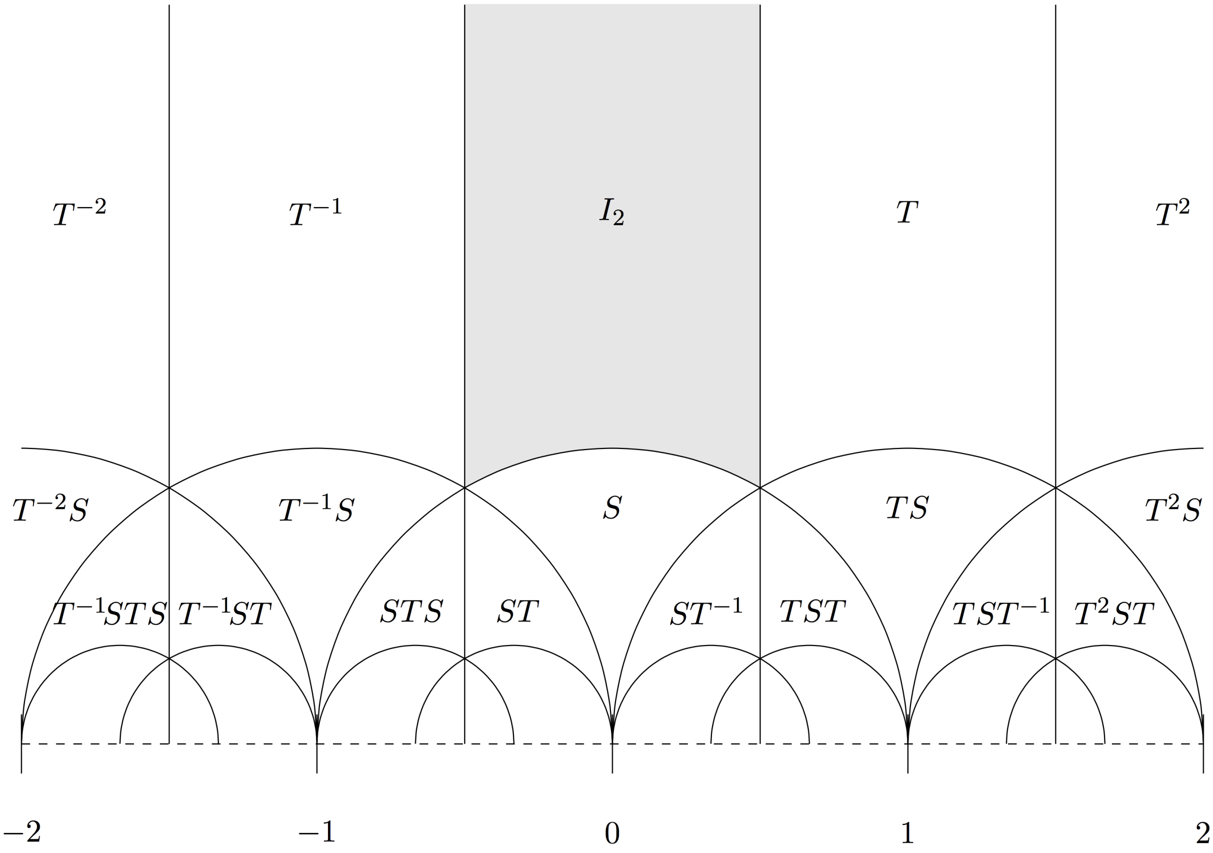

Figure 3: The fundamental domain of a modular form [5]

Essentially, the action of $SL_2(\mathbb{Z})$ on $\mathcal{H}$ maps the shaded region, the fundamental domain, to the entirety of $\mathcal{H}$, and the values of f must be consistent under this action. The proof and more details about this region are left to [15], Chapter VII.

We note that visually, the fundamental domain of the group $\Gamma_0(N)$ can be envisioned as taking N copies of the shaded region in Figure 3, rolling each one up, and "gluing" them together about a central point while working in projective space.

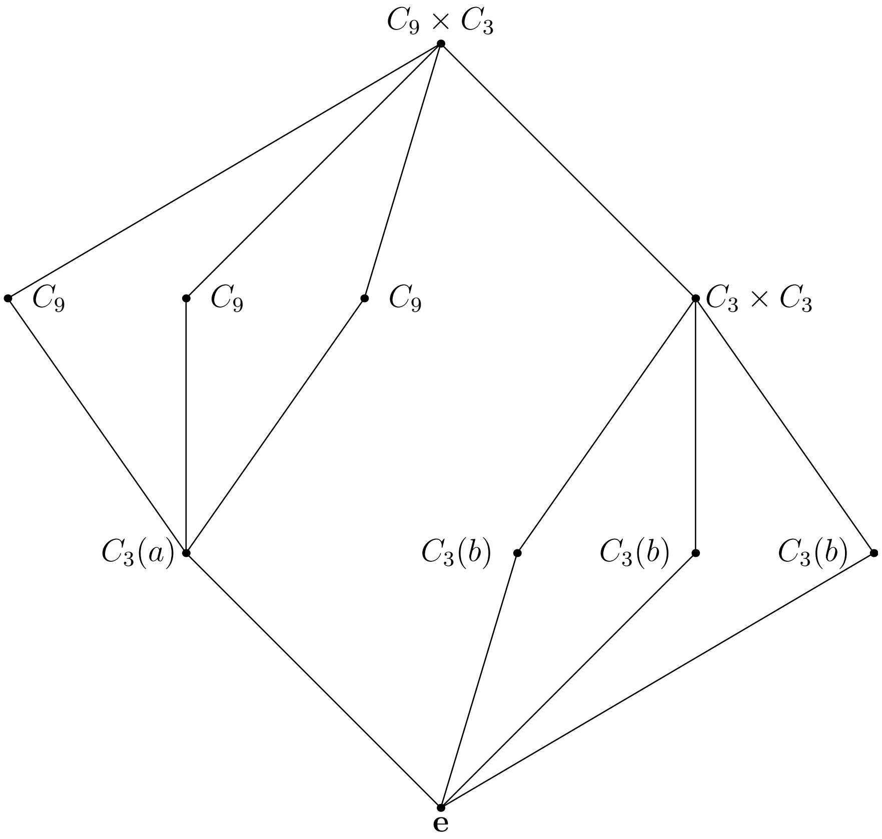

Figure 4: Poset diagram for subgroups of $C_9 \times C_3$.

The lattice structure of Figure 4 gives rise to Table 1.

Subgroup H	$\mathbb{P}(\geq H)$	$\mathbb{P}(= H)$
$C_9 \times C_3$	$\frac{1}{27}$	$\frac{1}{27}$
C_9	$\frac{1}{9}$	$\frac{1}{9} - \frac{1}{27} = \frac{2}{27}$
$C_3 \times C_3$	$\frac{1}{9}$	$\frac{1}{9} - \frac{1}{27} = \frac{2}{27}$
$C_3(a)$	$\frac{1}{3}$	$\frac{1}{3} - 4\left(\frac{2}{27}\right) - \frac{1}{27} = 0$
$C_3(b)$	$\frac{1}{3}$	$\frac{1}{3} - \frac{1}{9} = \frac{2}{9}$
$\mathbf{e}$	1	$1 - 3\left(\frac{2}{9}\right) - 4\left(\frac{2}{27}\right) - \frac{1}{27} = 0$

Table 1: Statistics for subgroups of $C_9 \times C_3$

B Proof of Lemma 4.2

First we state the definitions of an injective module and a divisible module.

Definition 10. A left R-module Q is *injective* if any of the following equivalent properties holds.

1. If Q is a submodule of some other left R-module M, then there exists another submodule K of M such that M is the internal direct sum of Q and K, i.e. $Q + K = M$ and $Q \cap K = \{0\}$.

2. If X and Y are left R-modules, $f : X \to Y$ is an injective module homomorphism and $g : X \to Q$ is an arbitrary module homomorphism, then there exists a module homomorphism $h : Y \to Q$ such that $hf = g$, i.e. the following diagram commutes.

$$\begin{tikzcd}
0 \arrow[r] & X \arrow[r, "f"] \arrow[d, "g"] & Y \arrow[dl, dashed, "h"] \\
& Q &
\end{tikzcd}$$

3. If $M \hookrightarrow N$, the natural map $\mathrm{Hom}(N, Q) \to \mathrm{Hom}(M, Q)$ is surjective.

4. Any short exact sequence $0 \to Q \to M \to K \to 0$ of left R-modules splits.

Definition 11. An R-module Q is *divisible* if for each $y \in Q$ and $r \in R$, $r \neq 0$, there exists some $z \in Q$ such that $rz = y$, i.e. each element of Q can be divided by each element of R.

Lemma B.1 (Lemma 4.2). *$\mathbb{C}^\times$ is an injective $\mathbb{Z}$-module.*

Proof. We note that $\mathbb{C}^\times$ is clearly a divisible $\mathbb{Z}$-module, and so it just remains to show that a divisible module over $\mathbb{Z}$ is also injective. It is well-known that to check injectivity over a principal ideal domain such as $\mathbb{Z}$, it suffices to check condition (1) of Definition 10 for X a sub-module of $\mathbb{Z}$ and $Y = \mathbb{Z}$ (see [12] p. 113). We use the terminology from condition (1) of Definition 10.

If X is an ideal of $\mathbb{Z}$, then $X = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. If $n = 0$, we may choose $h = g$, so assume $n \neq 0$. Since $\mathbb{C}^\times$ is divisible, we know there exists some $z \in \mathbb{C}^\times$ such that $z^n = g(n)$. Then we define $h : Y \to \mathbb{C}^\times$ by $1 \mapsto z$. Indeed, for any $tn \in X = n\mathbb{Z}$,

$$h(f(tn)) = h(tn) = z^{tn} = tg(n) = g(tn),$$

so h is the homomorphism that extends g, and $\mathbb{C}^\times$ is an injective $\mathbb{Z}$-module. □

C An Example Computation of k_H

Example 5. Consider the non-trivial inner twist ϵ that is defined by $p \mapsto \left(\frac{p}{7}\right)$, the Legendre symbol modulo 7.

This twist maps from $(\mathbb{Z}/7\mathbb{Z})^\times$ to $\{-1, 1\}$, which is the cyclic group of order 2 inside $\mathbb{C}^\times$. We view the characters ϵ as acting on $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ by associating each $n \in (\mathbb{Z}/7\mathbb{Z})^\times = \{1, 2, \ldots 6\}$ to the automorphism $\zeta_7 \mapsto \zeta_7^n$.

Then to find $K_{\{1,\epsilon\}} = K_H$, we want to find the field fixed under the elements of $(\mathbb{Z}/7\mathbb{Z})^\times$ that map to 1, the identity, under ϵ. These are those $p \in (\mathbb{Z}/7\mathbb{Z})^\times$ for which $\left(\frac{p}{7}\right) = 1$. The quadratic residues (mod 7) are 1, 2, and 4, and some computation shows that the field they fix is $\mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4)$. This extension is of degree 2, so $k_H = 2$.

Note that the group $H = \{1, \epsilon\}$ above is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which has size $2 = k_H$. This observation checks out with Theorem 3.3.

References

[1] R. Ash. Abstract Algebra: the Basic Graduate Year, 2002. [Online; accessed July 27, 2018].

[2] J. H. Bruinier, G. van der Geer, G. Harder, and D. Zagier. *The 1-2-3 of Modular Forms.* Springer-Verlag Berlin Heidelberg, 2008.

[3] T. Carrico. The Probability of Randomly Generating Finite Abelian Groups. *INVOLVE*, 6(4):431–436, 2013.

[4] K. Conrad. Characters of Finite Abelian Groups, 2018. [Online; accessed July 28, 2018].

[5] K. Conrad. SL(2,Z), 2018. [Online; accessed July 20, 2018].

[6] F. Diamond and J. Shurman. *A First Course in Modular Forms.* Springer Science + Business Media, 2005.

[7] M. (https://mathoverflow.net/users/27315/mf1). Field generated by the Fourier coefficients of a modular form. MathOverflow. URL:https://mathoverflow.net/q/131604 (version: 2013-05-23).

[8] A. Jackson. Interview with New AMS President Kenneth A. Ribet. *Notices of the American Mathematical Society*, 64(3):229–232, Mar. 2017.

[9] S. Kondo and T. Watari. String-theory Realization of Modular Forms for Elliptic Curves with Complex Multiplication. *arXiv:1801.07464 [hep-th]*, Jan. 2018.

[10] K. T.-L. Koo, W. Stein, and G. Wiese. On the generation of the coefficient field of a newform by a single Hecke eigenvalue. *Journal de théorie des nombres de Bordeaux*, 20(2):373–384, 2008.

[11] R. Langlands. Letter to Prof. Weil, 1967. [Online; accessed July 27, 2018].

[12] P. Ribenboim. *Classical Theory of Algebraic Numbers.* Springer Business+Science Media New York, 2001.

[13] K. A. Ribet. Twists of Modular Forms and Endomorphisms of Abelian Varieties. *Mathematische Annalen*, 253:43–62, 1980.

[14] K. A. Ribet and W. Stein. Lectures on Modular Forms and Hecke Operators, Jan. 2017. [Online; accessed July 31, 2018].

[15] J.-P. Serre. *A Course in Arithmetic.* Springer-Verlag New York, 1973.

[16] J. Siran and R. Jajcay. *Symmetries in Graphs, Maps, and Polytopes.* Springer International Publishing Switzerland, 2016.

[17] M. Viazovska. The sphere packing problem in dimension 8. *Annals of Mathematics*, 185(3):991–1015, Apr. 2017.

[18] S. A. J. Wiles. Modular Elliptic Curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3):443–551, 1995.