MODULAR FORMS MODULO 3 OF LEVEL 1

We describe the situation for $p = 3$ and $N = 1$ in detail. The first section introduces the space of modular forms and their Hecke algebra. The second section studies the associated Galois representation on this Hecke algebra. The third section states some preliminary results about the denisty of prime coefficients of certain modular forms mod 3. The results and methods here are inspired by work of Nicolas and Serre in [7, 8] and Bellaïche in [1], as well as unpublished work of Serre and Bellaïche, on modular forms mod 2.

1. Modular forms mod 3 and their Hecke algebra

1.1. **The space of forms.** Let $M_w(1, \mathbb{Z}_3)$ be the space of modular forms of weight w and level 1 with coefficients $\mathbb{Z}_3$, and $M_w \subset \mathbb{F}_3[\![q]\!]$ the image of $M_w(1, \mathbb{Z}_3)$ under the map "form q-expansions and reduce them modulo 3". Let $\widetilde{M} := \sum M_w \subset \mathbb{F}_3[\![q]\!]$ be the algebra of *all* modular forms mod 3 of level one. Swinnerton-Dyer observed in [12] that $\widetilde{M} = \mathbb{F}_3[\Delta]$, where Δ denotes the image of $q\prod(1-q^n)^{24}$ in $\mathbb{F}_3[\![q]\!]$.

The Hecke operators act on $f = \sum_n a_n(f)q^n \in \widetilde{M}$ in the usual way on q-expansions. For ℓ prime,

$$a_n(T_\ell f) = \begin{cases} a_{\ell n}(f) + \ell a_{n/\ell}(f) & \text{if } \ell \,|\, n \\ a_{\ell n}(f) & \text{otherwise.} \end{cases}$$

For $k \in \mathbb{Z}/3\mathbb{Z}$, define $M^k := \mathbb{F}_3\langle\, \Delta^i : i \equiv k \bmod 3 \,\rangle$, so that $\widetilde{M} = M^0 \oplus M^1 \oplus M^2$ is a $\mathbb{Z}/3\mathbb{Z}$-graded $\mathbb{F}_3$-algebra.

Proposition 1.

(1) *In fact,* $M^k = \{f \in \widetilde{M} : a_n(f) \neq 0 \implies n \equiv k \bmod 3\}$.
(2) *For* $\ell \neq 3$ *prime, the Hecke operator* T_ℓ *acts compatibly with the grading:* $T_\ell M^k \subset M^{\ell k}$.

Proof. To prove (1) for Δ, use the fact that Δ is an eigenform with $a_\ell(\Delta) = 1 + \ell$ for $\ell \neq 3$ prime (see Theorem below); the general case follows. For (2), use (1) and the happy accident that $\ell \equiv \ell^{-1} \bmod 3$. □

Therefore, $M := M^1 \oplus M^2 = \mathbb{F}_3\langle\, \Delta^n : 3 \nmid n \,\rangle$ is the kernel of U_3 and a $(\mathbb{Z}/3\mathbb{Z})^\times$-graded Hecke-invariant submodule of $\widetilde{M}$.

1.2. **The Hecke algebra.** Let A be the completed Hecke algebra generated by T_ℓ with $\ell \neq 3$ prime acting on M. More precisely, let $M_k = \mathbb{F}_3\langle\, \Delta^n : 3 \nmid n \text{ and } n \leq k\}$, let $A_k \subset \mathrm{End}_{\mathbb{F}_3}(M_k)$ be the algebra generated by the action of T_ℓ with $\ell \neq 3$ prime, and set $A = \varprojlim_k A_k$. The pairing $A \times M \to \mathbb{F}_3$ defined by $(T, f) \mapsto a_1(Tf)$ is nondegenerate and continous in the A-variable, so that A and M are continous duals of each other.

Theorem (Serre, [10], following Tate, [13])**.**
The only semisimple modular $\overline{\mathbb{F}}_3$*-representation of* $G_{\mathbb{Q},3}$ *is* $1 \oplus \omega$*, where* ω *is the mod-*3 *cyclotomic character.*

A number of facts follow:

(1) The only cuspidal eigenform in $\widetilde{M}$ is Δ, and $a_\ell(\Delta) = 1 + \ell$ for all primes ℓ prime to 3.
(2) Write T'_ℓ for the modified Hecke operator $T_\ell - a_\ell(\Delta)$. Then T'_ℓ acts locally nilpotently on M and $\widetilde{M}$: that is, T'_ℓ lowers Δ-degree of any form $f \in \widetilde{M}$ so that some power of it annihilates f.
(3) A is a complete local ring whose maximal ideal $\mathfrak{m}$ is generated by the modified Hecke operators T'_ℓ.

1.3. **The structure of A.** Following Bellaïche, define two sets of primes:

$$\mathcal{P}_x = \{\ell : \ell \equiv 2 \text{ or } 5 \bmod 9\} = \{\ell : \mathrm{Frob}_\ell \text{ generates } \mathrm{Gal}(\mathbb{Q}(\mu_9)/\mathbb{Q})\}$$

$$\mathcal{P}_y = \{\ell : \ell \equiv 1 \bmod 3, \text{ but 3 is not a cube mod } \ell\} = \{\ell : \mathrm{Frob}_\ell \text{ generates a 3-cycle in } \mathrm{Gal}(\mathbb{Q}(\mu_3, \sqrt[3]{3})/\mathbb{Q})\}.$$

Theorem (Bellaïche, appendix to [2], Theorem 24)**.** *There is a unique algebra isomorphism $\mathbb{F}_3[\![x,y]\!] \xrightarrow{\sim} A$ sending x to $T_2' = T_2$ and y to $T_7' = 1 + T_7$.*

For $\alpha \in \{x, y\}$, under this isomorphism we have $T_\ell' \equiv \alpha \mod \mathfrak{m}^2$ if and only if $\ell \in \mathcal{P}_\alpha$.

The proof explicitly computes the tangent space to the functor $D^0_{1+\omega}$ deforming the pseudocharacter $1+\omega$ to $\mathbb{F}_3$-algebras with fixed determinant to show that $\mathfrak{m}$ is generated by T_2 and $1+T_7$. To establish that $\dim A > 1$, Bellaïche proposes showing that the Hilbert-Samuel function $k \mapsto \dim_{\mathbb{F}_3} A/\mathfrak{m}^k$ grows *faster than linearly in k*; by duality, it suffices to prove the following

Lemma 2. *The nilpotence index $N_\ell(\Delta^n) := \min\{k : T_\ell'^{k+1}(\Delta^n) = 0\}$ grows slower than linearly in n.*

THIS LEMMA IS DISCUSSED IN DETAIL IN. Our proof crucially uses the linear recursion satisfied by the sequence $\{T_\ell'(\Delta^n)\}_n$, as well as the technical notion of *content* defined by Bellaïche. MAYBE DELETE THE REST The full statement recovers already-proved similar results for $p = 2$ and $p = 5$, but one hopes for more in the near future. The case $p = 2$ was first established with much greater precision (and more technical work) by Nicolas and Serre in [8]. The case $p = 5$ is a special case of a general theorem proved (using significantly more sophisticated methods) by Bellaïche and Khare in [2].

As a corollary, $A \simeq R^0_{1+\omega}$, the universal deformation ring representing $D^0_{1+\omega}$.

1.4. **The dual basis on M.** By the duality between M and A, given any isomorphism $\mathbb{F}_3[\![x,y]\!] \xrightarrow{\sim} A$, there is a unique basis $\{m(a,b); a, b \in \mathbb{N}\}$ of M *adapted to* the pair of generators (x, y) satisyfing

(1) If $a > 0$, then $x \cdot m(a,b) = m(a-1,b)$, and $x \cdot m(0,b) = 0$.
(2) If $b > 0$, then $y \cdot m(a,b) = m(a,b-1)$, and $x \cdot m(a,0) = 0$.
(3) $m(0,0) = \Delta$ and $a_1(m(a,b)) = 0$ unless $(a,b) = (0,0)$.

With a little linear algebra, we can compute elements of the basis $m(a,b)$ adapted to $(T_2, 1+T_7)$:

$$m(0,0) = \Delta \qquad m(1,1) = \Delta^{11} + 2\Delta^8 + 2\Delta^5$$
$$m(0,1) = 2\Delta^{10} + \Delta^7 \qquad m(2,0) = \Delta^{10} + 2\Delta^7 + \Delta^4$$
$$m(1,0) = \Delta^2 \qquad m(0,3) = 2\Delta^{82} + \Delta^{55} + \Delta^{34} + \Delta^{31} + \Delta^{25} + \Delta^{22} + 2\Delta^{19}$$
$$m(0,2) = \Delta^{28} + \Delta^{19} + 2\Delta^{16} + \Delta^{13} \qquad m(1,2) = 2\Delta^{29} + 2\Delta^{17} + 2\Delta^{14} + \Delta^8 + \Delta^5$$

A list of forms $m(a,b)$ adapted to $(T_2, 1+T_7)$ for $a + b \leq 17$, computed using SAGE, is available at `http://people.brandeis.edu/~medved/Data/mab3upto17.txt`.

1.5. **The grading on A.** From now on, we identify $A = \mathbb{F}_3[\![x,y]\!]$, where $x = T_2$ and $y = 1 + T_7$. We give A a $(\mathbb{Z}/3\mathbb{Z})^\times$-grading as follows: x is weighed 2 and y weighted 1, so that $A^1 = \mathbb{F}_3[\![x^2, y]\!]$, $A^2 = xA^1$.

Proposition 3.

(1) *For $\ell \neq 3$ prime, both T_ℓ and T_ℓ' are in A^ℓ, so that M is a graded A-module.*
(2) *If $X \in A^2 \cap (\mathfrak{m} - \mathfrak{m}^2)$ and $Y \in A^1 \cap (\mathfrak{m} - \mathfrak{m}^2)$ then $A = \mathbb{F}_3[\![X,Y]\!]$, with $A^1 = \mathbb{F}_3[\![X^2, Y]\!]$ and $A^2 = XA^1$.*

Call such pair (X,Y) graded parameters *for A. The element $m(a,b)$ of a basis adapted to (X,Y) is in M^{2ab}.*

(3) *If $\ell_x \in \mathcal{P}_x$ and $\ell_y \in \mathcal{P}_y$ are any two primes, then $(T_{\ell_x}, 1 + T_{\ell_y})$ is a pair of graded parameters for A.*

2. The Galois representation on the Hecke algebra

We construct and study the Galois pseudocharacter and representations carried by the Hecke algebra. In the first two subsections, we investigate the quotient of the Galois group through which everything factors. Then we closely study the Galois representation(s) on A and its specializations. Finally, we present an explicit matrix construction of the Galois representation.

2.1. **The Galois group of a residually reducible representation.** Let $p > 2$ be a prime. Let E_p be the maximal pro-p extension of $\mathbb{Q}(\mu_p)$ unramified outside p. Let $H_p = \mathrm{Gal}(E_p/\mathbb{Q}(\mu_p))$ and $G_p = \mathrm{Gal}(E_p/\mathbb{Q})$, so that we have an exact sequence

$$1 \to H_p \to G_p \to \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \to 1.$$

Any residually reducible modular representation of a level-1 form over $\overline{\mathbb{Q}}_p$ will factor through G_p.

Claim. *Let $f \in S_k(1, \overline{\mathbb{Q}}_p)$ be a cuspidal eigenform of level 1. Suppose that the associated Galois representation $\rho_f : G_{\mathbb{Q},p} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ is residually reducible when restricted to some invariant integral lattice. Then $\bar{\rho}_{f,\Lambda} : G_{\mathbb{Q},p} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ coming from any invariant lattice Λ factors through G_p.*

The next theorem of Shafarevich completely determines the structure of H_p in the case that p is regular.

Theorem (Shafarevich, [11], p. 82, example after Theorem 5)**.**
If p is a regular prime, then H_p is a free pro-p group on $\frac{p+1}{2}$ generators.

2.2. **The Galois group of interest in the case $p = 3$.**
We return to the case $p = 3$ and study the structure of $G = G_3$.

Set $H = H_3$. The exact sequence $1 \to H \to G \to \mathrm{Gal}(\mathbb{Q}(\mu_3)/\mathbb{Q}) \to 1$ splits by any choice of complex conjugation c lifting that of $\mathrm{Gal}(\mathbb{Q}(\mu_3)/\mathbb{Q})$. Shafarevich's theorem implies that G is a semidirect product $H \rtimes \{1, c\}$, where H is a free pro-3 group on 2 generators.

Definition (après Serre, unpublished work)**.** A profinite group Γ will be called a *group of type M_3* if Γ is topologically generated by two elements g and c with $c^2 = 1$ satisfying the following:

The closed subgroup generated by g and cgc is a free pro-3 group.

We'll call such a pair (g, c) a *pinning* of Γ. The subgroup $\Gamma^1 := \overline{\langle g, cgc \rangle}$ does not depend on the pinning. Its 3-Frattini quotient $\Gamma^1/\Phi_3(\Gamma^1)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and generated by the images of g and cgc.

If Γ is a group of type M_3 and (g, c) is a pinning, we define two subgroups of Γ. Let $\mathrm{Ab}(\Gamma) = [\Gamma, \Gamma]$ be the closed normal subgroup generated by $cgcg^{-1}$, and $\mathrm{Di}(\Gamma)$ be the closed normal subgroup generated by $cgcg$.

Claim. *Let Γ' be a topological group, and $\varphi : \Gamma \to \Gamma'$ a continous surjective homomorphism. Then*

1. *Γ' is an abelian group if and only if $\mathrm{Ab}(\Gamma) \subset \ker(\varphi)$*
2. *Γ' is a dihedral group if and only if $\mathrm{Di}(\Gamma) \subset \ker(\varphi)$.*

Both $\mathrm{Ab}(\Gamma)$ and $\mathrm{Di}(\Gamma)$ are independent of the pinning. Both are contained in Γ^1 and contain the derived subgroup $[\Gamma^1, \Gamma^1]$, so that the quotient of Γ^1 by either is abelian (and even cyclic, generated by the image of g).

If Γ is a group of type M_3 and (g, c) is a pinning of Γ, then for any n prime to 3, both (g^n, c) and (cg^nc, c) are also pinnings of Γ. More generally, (γ, c) is a pinning of Γ if and only if $\bar{c}\bar{\gamma}\bar{c}$ is not in the subgroup generated by $\bar{\gamma}$ in the quotient $\Gamma^1/\Phi_3(\Gamma^1)$.

Proposition 4. *The Galois group G is of type M_3. A pinning is given by (g, c) where c is any complex conjugation, and g is an element of H whose images generate both* $\mathrm{Gal}\left(\mathbb{Q}(\mu_9)/\mathbb{Q}(\mu_3)\right)$ *and* $\mathrm{Gal}\left(\mathbb{Q}(\mu_3, \sqrt[3]{3})/\mathbb{Q}(\mu_3)\right)$.

In particular, if $c \in G$ be any complex conjugation, and $\ell \equiv 4$ or $7 \bmod 9$ is a prime with 3 is not a cube modulo ℓ, then (Frob_ℓ, c) *is a pinning of G. This includes $\ell = 7, 13, 31, 43, 79, 97$.*

Proof. Note that the 3-Frattini quotient of $H = G^1$ is $\mathrm{Gal}(\mathbb{Q}(\mu_9, \sqrt[3]{3})/\mathbb{Q}(\mu_3))$. □

2.3. **The Galois pseudocharacter carried by A.**
This section and the next closely follow Bellaïche's treatment in [1] of the case $p = 2$.

As before G is the Galois group of the maximal pro-3 extension of $\mathbb{Q}(\mu_3)$ unramified away from the 3 over $\mathbb{Q}$. Let $G^1 = H$ and $G^2 = G - H$. Also, $A = \mathbb{F}_3[\![x, y]\!]$ is the completed Hecke algebra acting on M, with the grading $A^1 = \mathbb{F}_3[\![x^2, y]\!]$ and $A^2 = x\mathbb{F}_3[\![x^2, y]\!]$.

In general, a *continuous pseudocharacter of dimension* 2 of a group Γ to a topological ring $B \ni \frac{1}{2}$ is a continuous map $t : \Gamma \to B$ designed to mimick the algebraic behavior of the trace of a two-dimensional representation of Γ over B. Specifically, for all $g, h \in \Gamma$, we have $t(gh) = t(hg)$ — that is, t is *central* — and

$$t(gh) + d(g)t(g^{-1}h) = t(g)t(h),$$

where $d = \det t : \Gamma \to B^\times$ is the map $d(g) = \frac{t(g)^2 - t(g^2)}{2}$.

Pseudocharacters have been studied by Rouquier in [9] and Chenevier in [4], where they are called *determinants*. In any case, the notions is equivalent in this case, and intentionally intertwined here.

Proposition 5.

(1) *There is a unique continuous pseudocharacter $t : G \to A$ satisfying $t(\mathrm{Frob}_\ell) = T_\ell$ for $\ell \neq 3$ prime. Its determinant* $\det(t) = \omega$. *Moreover,*
   (a) *For $i \in (\mathbb{Z}/3)^\times$, we have $t(G^i) \subset A^i$.*
   (b) *If (g, c) is a pinning of G, then $(t(cg), 1 + t(g))$ is graded pair of parameters for A.*

(2) *There exists a unique representation $r : G \to \mathrm{GL}_2(\mathrm{Frak}\, A)$ satisfying* $\mathrm{tr}\, r(\mathrm{Frob}_\ell) = T_\ell$ *for $\ell \neq 3$ prime. Its determinant is ω. It is absolutely irreducible.*

The construction of t is a standard one. The compatibility of t with the grading follows from the Chebotarev density theorem since we already know that $T_\ell \in A^\ell$. The existence of r over $\overline{\mathrm{Frak}\, A}$ follows from the theory of pseudocharacters. This representation descends to $\mathrm{Frak}\, A$ because it is odd. It is absolutely irreducible because A is the universal deformation ring of $\bar{t} = 1 + \omega$, and, for example, Bellaïche gives an irreducible deformation of $\bar{t}$ to $\mathbb{F}_3[\varepsilon]$ factoring through $\mathrm{Gal}(\mathbb{Q}(\mu_3, \sqrt[3]{3})/\mathbb{Q})$ in [2].

2.4. **The specializations of the Galois representations on A.** Choose a free G-stable lattice Λ of r_K. Write r_Λ for the action of G on Λ and $r_{\Lambda,B}$ for the action of G on $\Lambda \otimes B$ for any extension $A \to B$ of rings. Write $r_{\Lambda,\mathfrak{p}}$ for $r_{\Lambda,k(\mathfrak{p})}$, where $\mathfrak{p} \subset A$ is a prime ideal and $k(\mathfrak{p})$ is its residue field, and $r_\mathfrak{p}^{\mathrm{ss}}$ for its semisimplification. Suppress Λ from notation whenever the relevant object doesn not depend on it. Use the same notation conventions for t.

We already know that $r_{(0)} = r$ is absolutely irreducible, and that $r_\mathfrak{m}^{\mathrm{ss}} = 1 \oplus \omega$. We study $r_{\Lambda,\mathfrak{m}}$ and $r_{\Lambda,\mathfrak{p}}$ for primes $\mathfrak{p}$ of height 1, which are all principal. Let $\mathfrak{p}_0 \subset A$ be the prime ideal generated by

$$y - P_\alpha(x^2) + 2 = y - x^2 - x^{10} + x^{12} - x^{14} - x^{16} + O(x^{28}),$$

where $\alpha = \frac{\log_3 7}{\log_3 4} \in \mathbb{Z}_3$ with $\log_3$ the 3-adic logarithm, and $P_\alpha \in \mathbb{F}_3[\![u]\!]$ is the power series satisifying $P_\alpha(z + z^{-1} - 2) = z^\alpha + z^{-\alpha}$. Recall that H is the index-2 subgroup of G.

Theorem 6.

(1) *The residual representation $r_{\Lambda,\mathfrak{m}}$ is indecomposable. Moreover, $r_{\mathfrak{m}}|_H \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ is a nontrivial extension in $\mathrm{H}^1_{\mathrm{cont}}(H, \mathbb{F}_3) = \mathrm{Hom}_{\mathrm{cont}}(H, \mathbb{F}_3)$ corresponding to $\mathrm{Gal}(\mathbb{Q}(\mu_3, \sqrt[3]{3})/\mathbb{Q}(\mu_3))$.*

(2) *If $\mathfrak{p} \neq \mathfrak{p}_0$ is a prime of height 1, then $r_{\mathfrak{p}}$ is absolutely irreducible. If further $\mathfrak{p} \neq (x)$, then $r_{\mathfrak{p}}$ is strongly absolutely irreducible: it stays absolutely irreducible restricted to any finite-index subgroup of G.*

(3) *The represenation $r_{\Lambda,\mathfrak{p}_0}$ is reducible over $A/\mathfrak{p}_0 \subset k(\mathfrak{p}_0)$. Its trace is $t_{\mathfrak{p}_0} = \chi + \omega\chi^{-1}$, where $\chi : G^{\mathrm{ab}} = \mathbb{Z}_3^\times \to (A/\mathfrak{p}_0)^\times = \mathbb{F}_3[\![x]\!]^\times$ is the continuous character defined by $\chi(\mathrm{Frob}_2) = -x + \sqrt{1+x^2}$.*

(4) *The image of $r_{\Lambda,(x)}$ is dihedral, and $r_{\Lambda,(x)} = \mathrm{Ind}_H^G \psi$, where ψ is a character of $H/\mathrm{Di}(G)$ defined over a quadratic extension of $A/(x) = \mathbb{F}_3[\![y]\!]$ and characterized by setting $\psi(\mathrm{Frob}_7) = -y \pm \sqrt{y+y^2}$. In particular $r_{\Lambda,(x)}\,|_H = \psi + \psi^{-1}$ is irreducible over $k\big((x)\big)$.*

Corollary 7. *Up to A-isomorphism, there are exactly two G-representations $r^\pm : G \to \mathrm{GL}_2(A)$ satisfying $\mathrm{tr}\, r^\pm(\mathrm{Frob}_\ell) = T_\ell$ for $\ell \neq 3$ prime, distinguished by $r^+_{\mathfrak{m}} \sim \begin{pmatrix} 1 & * \\ 0 & \omega \end{pmatrix}$ and $r^-_{\mathfrak{m}} \sim \begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$. Both satisfy $\mathrm{tr}(r^\pm) = t$ and $\det(r^\pm) = \omega$. They are isomorphic over K.*

Proof. Let V be the representation r_K. Any A-representation r satisfying $\mathrm{tr}\, r(\mathrm{Frob}_\ell) = T_\ell$ must become isomorphic to V when base-changed to K, so we may view any such as a free G-stable A-lattice inside V. Let Λ' and Λ be two such; since they are reflexive, they are completely determined by their localizations at height-1 primes. For almost every such $\mathfrak{p}$, we always have $\Lambda_{\mathfrak{p}} = \Lambda'_{\mathfrak{p}}$ a priori, so we may scale Λ' by an element of K to guarantee $\mathfrak{p}\Lambda \subsetneq \Lambda' \subset \Lambda$ for all $\mathfrak{p}$. But now for $\mathfrak{p} \neq \mathfrak{p}_0$, we have $r_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}/\mathfrak{p}\Lambda_{\mathfrak{p}}$ irreducible, so that $\Lambda_{\mathfrak{p}} = \Lambda'_{\mathfrak{p}}$. Finally, $\Lambda_{\mathfrak{p}_0}/\mathfrak{p}_0\Lambda_{\mathfrak{p}_0}$ is reducible but not indecomposable, so there are exactly two choices for $\Lambda'_{\mathfrak{p}_0}$: either $\Lambda'_{\mathfrak{p}_0} = \Lambda_{\mathfrak{p}_0}$, or $\Lambda'_{\mathfrak{p}_0}/\mathfrak{p}\Lambda_{\mathfrak{p}_0}$ is the G-invariant line in $r_{\Lambda,\mathfrak{p}_0}$, and the two choices will alter which mod-$\mathfrak{m}$ character appears as the invariant sub. Therefore both occur. See [3] for the theory of reflexive modules over a noetherian normal domain. □

2.5. **The Galois representation over A explicitly.** We give an explicit matrix realization of the representations analyzed in the previous section with respect to a pinning of G. The construction is directly inspired by a similar explicit construction of Serre for $p = 2$ of the representation defined by Bellaïche in [1]. Serre credits W. Goldman's exposition of work of Fricke and Vogt for the particular matrices: see [6].

Let Γ be a group of type M_3 with pinning (g, c), and let $B = \mathbb{F}_3[\![x, y]\!]$ be an abstract power series ring with $\mathfrak{m}_B$ its maximal ideal. Let $\alpha^\pm \in B$ be two elements satisfying $\alpha^{-1} - \alpha = x$. Namely,

$$\alpha^\pm = x \pm \sqrt{1+x^2} = x \pm (1 - x^2 + x^4 + x^6 - x^8 + x^{10} + x^{18} + \cdots).$$

For $\alpha = \alpha_+, \alpha_-$, define three matrices in $\mathrm{GL}_2(B)$:

$$M_g = \begin{pmatrix} y-1 & -1 \\ 1 & 0 \end{pmatrix}, \qquad M_h = \begin{pmatrix} 0 & \alpha^{-2} \\ -\alpha^2 & y-1 \end{pmatrix}, \qquad M_c = \begin{pmatrix} 0 & \alpha^{-1} \\ \alpha & 0 \end{pmatrix}.$$

Proposition 8. *For each choice of α, the map $\rho : \Gamma \to \mathrm{GL}_2(B)$ defined by $\rho(g) = M_g$, $\rho(cgc) = M_h$, and $\rho(c) = M_c$ defines a continuous representation. Moreover, ρ^+ and ρ^- are isomorphic over $\mathrm{Frak}\, B$ but not over B.*

Proof. Check that $M_c^2 = 1$ and $M_c M_g M_c = M_h$. And modulo $\mathfrak{m}_B$ we see that $\overline{M}_g = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ and $\overline{M}_h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ land in the same order-3 subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$, which means that M_g and M_h lie in some

pro-3 subgroup of $\mathrm{SL}_2(B)$, so that ρ extends continuously to H and then to G. One can check explicitly that the matrix $X = \begin{pmatrix} \alpha^2(y-1) & -1-\alpha^2) \\ 1+\alpha^2 & -y+1 \end{pmatrix}$ intertwines ρ^+ and ρ^-, but $\det X \equiv -y \bmod \mathfrak{m}_B^2$, so that $X \notin \mathrm{GL}_2(B)$. □

One can also check explicitly the following:

(1) $\rho^+_{\mathfrak{m}_B}$ is the nonsplit extension of nontrivial character of Γ/Γ^1 by the trivial character, and $\rho^-_{\mathfrak{m}_B}$ is the nonsplit extension of same characters in the other order.
(2) $\rho_{B/I}$ is reducible if and only if $I \supset \big(y + y^2 - x^2\big) = \big(y - 1 + \sqrt{1+x^2}\big)$.
(3) $\rho_{B/I}\big|_{\Gamma^1}$ is reducible if and only if $I \supset \big(y + y^2 - x^2\big)$ or $I \supset \big(x\big)$.

We now return to our Galois group G and our Hecke algebra H.

Corollary 9. *For any pinning (g, c) of G the two represenations $r^\pm$ from Corollary 7 can be realized explicitly:*

$$r^\pm(g) = \begin{pmatrix} t(g) & -1 \\ 1 & 0 \end{pmatrix}, \qquad r^\pm(cgc) = \begin{pmatrix} 0 & (\alpha^\pm)^{-2} \\ -(\alpha^\pm)^2 & t(g) \end{pmatrix}, \qquad r^\pm(c) = \begin{pmatrix} 0 & (\alpha^\pm)^{-1} \\ \alpha^\pm & 0 \end{pmatrix}.$$

Here $\alpha^\pm = t(cg) \pm \sqrt{1 + t(cg)^2} \in A$.

Proof. A semisimple continous representation of Γ whose determinant is the nontrivial character of Γ/Γ^1 over a field K is defined uniquely by the K-triple $(\mathrm{tr}(g), \mathrm{tr}(c), \mathrm{tr}(cg))$: a consequence of the pseudocharacter identity. □

3. Density of prime coefficients of forms mod 3

In this section, we state some partial results and conjectures about the distribution of prime coefficients of modular forms modulo 3. The section is inspired by unpublished work of Bellaïche on modular forms mod 2.

Recall that $G = \mathrm{Gal}(E/\mathbb{Q})$, where E is the maximal pro-3 extension of $\mathbb{Q}(\mu_3)$ unramified outside 3.

For a form $f \in M$ and $i \in \mathbb{F}_3$, the set $\mathcal{P}(f, i) = \{\ell \text{ prime} : a_\ell(f) = i\}$ is *frobenian*: there exists a number field K so that whether $\ell \in \mathcal{P}(f, i)$ depends only on the conjugacy class of Frob_ℓ in $\mathrm{Gal}(K/\mathbb{Q})$. Indeed, the pseudocharacter $t_f : G \to A \to A/\operatorname{ann}(f)$ is continuous with finite image, so that it factors through a finite extension, and one can show that a subfield $K \subset E$ is *frobenian for f* — that is, $a_\ell(f)$ depends only $\mathrm{Frob}_\ell^{K/\mathbb{Q}}$ — if and only if t_f factors through K. The minimal frobenian field for f will be denoted K_f: it is the fixed field of the closed normal subgroup $\ker t_f \subset G$.

Let $\delta(f, i)$ be the Dirichlet density of the set $\mathcal{P}(f, i)$; it is always a rational number, an integer divided by $2 \cdot 3^k$. Write $\delta(f)$ for the unit-sum tuple $\big(\delta_0(f), \delta_1(f), \delta_2(f)\big)$. For example, since $a_\ell(\Delta) = \ell + 1$ for all ℓ except 3, the density of Δ is $\delta(\Delta) = (\frac{1}{2}, 0, \frac{1}{2})$. Using SAGE, we estimate:

$$\begin{aligned} \delta(\Delta^2) &= (\tfrac{2}{3}, \tfrac{1}{6}, \tfrac{1}{6}) & \qquad \delta(\Delta^8) &= (\tfrac{2}{3}, \tfrac{1}{6}, \tfrac{1}{6}) \\ \delta(\Delta^4) &= (\tfrac{2}{3}, \tfrac{1}{3}, 0) & \qquad \delta(\Delta^{10}) &= (\tfrac{7}{9}, \tfrac{1}{9}, \tfrac{1}{9}) \\ \delta(\Delta^5) &= (\tfrac{2}{3}, \tfrac{1}{6}, \tfrac{1}{6}) & \qquad \delta(\Delta^{11}) &= (\tfrac{2}{6}, \tfrac{1}{6}, \tfrac{1}{6}) \\ \delta(\Delta^7) &= (\tfrac{2}{3}, \tfrac{2}{9}, \tfrac{1}{9}) & \qquad \delta(\Delta^{13}) &= (\tfrac{2}{3}, \tfrac{5}{27}, \tfrac{4}{27}) \end{aligned}$$

Futher computations suggest that $\delta(\Delta^n) = (\frac{2}{3}, \frac{1}{6}, \frac{1}{6})$ for all n with $13 < n < 5000$. Since M has a grading that forces $a_\ell(\Delta^n) = 0$ unless $\ell \equiv n \bmod 3$, a density of $(\frac{2}{3}, \frac{1}{6}, \frac{1}{6})$ for a homogeneous form is in an equidistribution of prime coefficients among the elements of $\mathbb{F}_3$. But what about the other patterns?

3.1. **The density of abelian and dihedral forms.** A form $f \in M$ will be called *abelian* if the map $\ell \mapsto a_\ell(f)$ depends on the congruence class of ℓ modulo some integer N, here necessarily always a power of 3. Equivalently, f is abelian if and only if f its minimal frobenian field K_f is an abelian extension of $\mathbb{Q}$. Similarly, $f \in M$ will be called *dihedral* if K_f is a dihedral extension of $\mathbb{Q}$.

Theorem 10. *Let $f \in M$ be a modular form.*

(1) *f is abelian if and only if f is annihilated by $\mathfrak{p}_0$, the* ideal of abelianness.
(2) *f is dihedral if and only if f is annihilated by (x), the* ideal of dihedralness.

One direction is established with Theorem 6. The other requires some explicit computations with $\ker t_f$ and the subgroups $\mathrm{Ab}(G)$ and $\mathrm{Di}(G)$.

The space of dihedral forms has a obvious basis $\{m(0,n)\}_{n\geq 0}$ with respect to any pair of graded parameters. Abelian forms are less tractible, but for any pair of graded parameters (X,Y), one can still construct a unique basis $\{ab(n)\}_{n\geq 0}$ with $ab(n)$ homogeneous and contained in $m(n,0)+M[\mathfrak{m}^n]$, with $X\cdot ab(n) = ab(n-1)$ for $n>0$, and with $ab(0)=\Delta$. Here are a few abelian forms adapted to $(T_2, 1+T_7)$, first computed by Paul Monsky:

$$\begin{aligned}
ab(0) &= m(0,0) && = \Delta & \qquad ab(3) &= m(3,0)+m(1,1) && = -\Delta^5\\
ab(1) &= m(1,0) && = \Delta^2 & \qquad ab(4) &= m(4,0)+m(2,1)+m(0,2) && = -\Delta^{10}\\
ab(2) &= m(2,0)+m(0,1) && = -\Delta^4 & \qquad ab(5) &= m(5,0)+m(3,1)+m(1,2) && = \Delta^{11}+\Delta^8+\Delta^5
\end{aligned}$$

In other words, for both abelian and dihedral forms, the dimension of the subspace annihilated by $\mathfrak{m}^n$ is n. Since we know by Lemma 2 that $\dim M[\mathfrak{m}^n]$ grows faster than linearly, we can say that generically a form is not in the span of the dihedral and abelian forms.

Proposition 11. *The only n for which $\Delta^n \in M$ is dihedral is $n = 1, 2$.*

The proof uses Derksen's algorithm for computing the zeros of a linear recurrence sequence in characteristic p by constructing a p-automaton (see [5]) and the T_2-recursion $T_2(\Delta^n) = \Delta\, T_2(\Delta^{n-2}) - \Delta^3\, T_2(\Delta^{n-3})$.

Conjecture 1. *The only n for which $\Delta^n \in M$ is abelian is $n = 1, 2, 4, 5, 10$.*

Theorem 12. *Let (g,c) be a pinning of G, and let $m_{(g,c)}(a,b)$ be the basis adapted to the graded pair $(t(cg), t(g)-2)$. Let $f \in m_{(g,c)}(n,0) + M[\mathfrak{m}^n]$ be a homogeneous abelian form. Let k be the number of digits in the base-3 expansion of n, with z being the number of 0s and u the number of 1s. Let $v = v_3(n)$ be the 3-valuation of n.*

$$\text{Then } \begin{cases}
\delta(f,1) = \delta(f,2) = \dfrac{2^{u-1}\,3^z}{2\cdot 3^k} & \text{if the last nonzero digit of } n \text{ is } 1\\[2ex]
\delta(f,1) = \delta(f,2) = \dfrac{2^{u-1}\,(3^z+3^{z-v})}{2\cdot 3^k} & \text{if the last nonzero digit of } n \text{ is } 2 \text{ and } u>0\\[2ex]
\delta(f,1) = \dfrac{2\cdot 3^{z-v}}{2\cdot 3^k} \text{ and } \delta(f,2) = \dfrac{3^z-3^{z-v}}{2\cdot 3^k} & \text{if } u = 0.
\end{cases}$$

Sketch of proof. One proves explicitly that $\mathrm{Gal}(K_f/\mathbb{Q}) = C_{2\cdot 3^k}$, generated by $h = cg$. Let $Q_m(X) \in \mathbb{F}_3[X]$ be the polynomial satisfying $Q_m(z-z^{-1}) = z^m - z^{-m}$; then $t(h^m) = Q_m(t(h))$. By Chebotarev,

$$\delta(f,i) = \frac{\#\{m : a_1(t(h^m)f) = i\}}{2\cdot 3^k}.$$

Since $f = m(n,0) + (\text{terms killed by } t(h)^n)$, we see that $a_1(t(h^m)f) = [X^n]Q_m(X)$, the X^n-coefficient of Q_m. The rest is a bit of drudgerous combinatorial computations. □

A similar result is true for dihedral forms, governed by coefficients of $P_m(X)$, defined before Theorem 6.

Conjecture 2. *If f is homogeneous and not in the span of abelian or dihedral forms, then $\delta(f) = (\frac{2}{3}, \frac{1}{6}, \frac{1}{6})$.*

References

[1] Bellaïche, J. Une représentation galoisienne universelle attachée aux formes modulaires modulo 2. *Comptes rendus mathématique. Académie des Sciences. Paris 350* (2012).

[2] Bellaïche, J., and Khare, C. Level 1 Hecke algebras of modular forms modulo p. To appear in *Compositio*. Available at `http://people.brandeis.edu/~jbellaic/preprint/Heckealgebra6.pdf`.

[3] Bourbaki, N. *Algèbre Commutative*. Chapter 7, Section 4.3, Theorem 3.

[4] Chenevier, G. The p-adic analytic space of pseudocaracters of a profinite group and pseudorepresenations over arbitrary rings. In *Proceedings of the LMS Durham Symposium: Automorphic forms and Galois representations* (2011). Available at `http://gaetan.chenevier.perso.math.cnrs.fr/articles/determinants.pdf`.

[5] Derksen, H. A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. *Invent. Math. 168*, 1 (2007), 175–224.

[6] Goldman, W. An exposition of results of Fricke and Vogt. `http://arxiv.org/pdf/math/0402103.pdf`.

[7] Nicolas, J.-L., and Serre, J.-P. Formes modulaires modulo 2 : l'ordre de nilpotence des opérateurs de Hecke modulo 2. *Comptes rendus mathématique. Académie des Sciences. Paris 350* (2012).

[8] Nicolas, J.-L., and Serre, J.-P. Formes modulaires modulo 2 : structure de l'algèbre de Hecke. *Comptes rendus mathématique. Académie des Sciences. Paris 350* (2012).

[9] Rouquier, R. Caractérisation des caractères et pseudo-caractères. *Journal of Algebra 180*, 2 (1996), 571–586.

[10] Serre, J.-P. *Œuvres. Vol. III*. Springer-Verlag, Berlin, 1986, p. 710. Note 229.2.

[11] Shafarevich, I. R. Extensions with prescribed ramification points. *Publications Mathématiques de l'IHES*, 18 (1963), 71–95.

[12] Swinnerton-Dyer, H. P. F. On l-adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*. Springer, Berlin, 1973, pp. 1–55. Lecture Notes in Math., Vol. 350.

[13] Tate, J. The non-existence of certain Galois extensions of $\mathbb{Q}$ unramified outside 2. In *Arithmetic geometry (Tempe, AZ, 1993)*, vol. 174 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1994, pp. 153–156.