

THREE-DIMENSIONAL IMPRIMITIVE REPRESENTATIONS OF THE MODULAR GROUP AND THEIR ASSOCIATED MODULAR FORMS

CAMERON FRANCO AND GEOFFREY MASON

ABSTRACT. This paper uses previous results of the authors [6] to study certain noncongruence modular forms. We prove that these forms have unbounded denominators, and in certain cases we verify congruences of Atkin–Swinnerton-Dyer type [2] satisfied by the Fourier coefficients of these forms. Our results rest on group-theoretic facts about the modular group Γ , a detailed study of imprimitive three-dimensional representations of Γ , and the theory of their associated vector-valued modular forms. For the proof of the congruences we also make essential use of a result of Katz [7].

CONTENTS

1. Introduction	1
2. Imprimitive representations of dimension 3	3
3. Geometric considerations	8
4. Vector-valued modular forms of minimal weight	13
5. Unbounded denominators in the general case	17
6. Congruences	19
References	23

1. INTRODUCTION

The main purpose of this paper is to study arithmetic properties of the Fourier coefficients of a class of noncongruence modular forms. In a ‘top-down’ approach to the general problem, one takes a finite-index subgroup G of $\Gamma := \mathrm{PSL}_2(\mathbf{Z})$ and considers the spaces of weight k modular forms $M_k(G, \chi)$ for characters $\chi : G \rightarrow \mathbf{C}^*$ of finite order. The kernel $H = \ker \chi$ is typically a *noncongruence* subgroup of Γ , and a form $f \in M_k(G, \chi)$ is typically a noncongruence modular form on H . The largest subgroups G (i.e., those of least index in Γ) which actually give rise to noncongruence forms in this manner are the nonnormal subgroups of Γ of index 3. These are conjugate to $\bar{\Gamma}_0(2)$ (for notation, see below), and it is this case that we are concerned with here.

In a well-known paper [2], Atkin–Swinnerton-Dyer made perhaps the first detailed study of the Fourier coefficients of noncongruence forms. They examined several general phenomenon, including so-called *unbounded denominators* and *ASD-type congruences*. Their observations have inspired many interesting results, cf. [1], [8], [9], [10],

[11], [12], [17]. In the present paper, we give a general proof of the unbounded denominators conjecture for noncongruence forms in $M_k(\bar{\Gamma}_0(2), \chi)$, and prove ASD-type congruences in certain cases.

We describe some of our results. The finite-order characters $\chi = \chi_{n,\varepsilon}$ of $\bar{\Gamma}_0(2)$ are conveniently labelled by a positive integer n and a sign $\varepsilon = \pm 1$. With this notation, it transpires that $\ker \chi$ is congruence if, and only if, $n|24$ (Theorem 5). We will show (Theorem 21) that if $f \in M_k(\bar{\Gamma}_0(2), \chi)$ is any nonzero holomorphic modular form with algebraic Fourier coefficients, and if $p|n$ is a prime, then the powers of p that divide the denominators of f are *unbounded* under any of the following circumstances: $p \geq 5$; $p = 3$ and $p^2|n$; $p = 2$ and $p^4|n$.

The modular curves $X_H := H \backslash \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$ defined by $\ker \chi$ and related groups are of interest in themselves. For example, we will show that if n is odd and $\varepsilon = -1$ then X_H is a hyperelliptic curve (noncongruence unless $n|24$) given by the affine equation $y^2 = x^n + 64$. (See Theorems 12 and 16 for more complete results). This leads to ASD-style 3-term congruences for primes $p \equiv -1 \pmod{n}$ satisfied by the coefficients of a basis of holomorphic differentials on X_H .

The methods that we use to establish these results, advertised and illustrated (in the congruence setting) in a forthcoming paper [6], are likely to be unfamiliar to many readers, and we will say something about them here. Given any form $f \in M_k(\bar{\Gamma}_0(2), \chi)$ as above, there is a 3-dimensional *vector-valued modular form* (vvmf) $F := {}^t(f_1, f_2, f_3)$ whose components f_i are the forms $f|_k \gamma_i$, γ_i ranging over cosets representatives of $\bar{\Gamma}_0(2) \backslash \Gamma$. Such an F satisfies the transformation law

$$(1) \quad F|_k \gamma(\tau) = \rho(\gamma)F(\tau) \quad (\gamma \in \Gamma),$$

where $\rho := \text{Ind}_{\bar{\Gamma}_0(2)}^{\Gamma} \chi$ is the 3-dimensional representation of Γ obtained by *inducing* χ , and sits in the weight k graded piece of the space

$$\mathcal{H}(\rho) = \bigoplus_{k \geq k_0} \mathcal{H}_k(\rho)$$

of all holomorphic vector-valued modular forms on Γ that transform as in (1) for some weight k . With the harmless assumption that ρ is *irreducible* (equivalently, $n \neq 1$ or 3), the lowest nonzero weight space is 1-dimensional, and a good proportion of our effort is expended on understanding the nature of a spanning form $F_0 \in \mathcal{H}_{k_0}(\rho')$ where ρ' is a representation *equivalent* to ρ with the property that $\rho'(\bar{T})$ is *diagonal*. Some techniques from the theory of vector-valued modular forms (described in [6]) show that the 3 components of the weight zero vvmf F_0/η^{2k_0} span the solution space of a Fuchsian equation. This leads to the situation that the components of F_0 (and then also the components of *every* vvmf in $\mathcal{H}(\rho)$ such as the f that we started with) can be described in terms of classical forms of level 1 and hypergeometric series ${}_3F_2(a, a+1/3, a+2/3; a-b+1, a-c+1; K)$. Here, $K = 1728j^{-1}$ with j the absolute modular invariant, and a, b, c depend on the eigenvalues of $\rho(\bar{T})$.

The technique of relating components of vector-valued modular forms to hypergeometric series in order to study the question of unbounded denominators was used in [5], where the 2-dimensional case was completely settled. However, in that setting one does not encounter noncongruence modular forms. Chris Marks first studied the 3-dimensional case in [14], and obtained results about unbounded denominators for vector-valued modular forms of large enough weight.

The paper is organized as follows. In Section 2 we treat the characters χ of $\bar{\Gamma}_0(2)$ and their induced representations, and in particular we determine when $\ker \rho$ is congruence. In Section 3 we deal with the modular curves defined by $\ker \chi$ and related groups, establishing that the curves we are interested in are hyperelliptic. In Section 4 we make a detailed study of the Fourier coefficients of the components of the lowest weight vvmf F_0 . These are products of a power of η , a power of K , and a hypergeometric series of type ${}_3F_2$, and we show that each component of F_0 satisfies the unbounded denominator statement of Theorem 21. In Section 5, we establish the general unbounded denominator result of Theorem 21 by showing how it follows from the special case of F_0 together with some further general theory of vector-valued modular forms. In Section 6 we establish ASD-type congruences for forms in $S_{k_0}(H, \chi)$ in certain cases when $k_0 = 2$. Having available the explicit equation $y^2 = x^n + 64$ for the curves makes the zeta function accessible, and we can ultimately appeal to a theorem of Katz [7]. Interestingly, this approach *eschews* our explicit formulas for the forms in terms of hypergeometric series. It would be of interest to find a proof of our congruences using hypergeometric series in place of [7].

2. IMPRIMITIVE REPRESENTATIONS OF DIMENSION 3

We use the following notation: $\Gamma := \mathrm{PSL}_2(\mathbf{Z})$, and if M is either an element or a subgroup of $\mathrm{SL}_2(\mathbf{Z})$ then \bar{M} denotes its image in Γ . Thus $\bar{\Gamma}(n)$ and $\bar{\Gamma}_0(n)$ are the images of the usual congruence subgroups $\Gamma(n)$ and $\Gamma_0(n)$ in Γ . Given any group G , the notation G' denotes the commutator subgroup of G . We make use of the following elements of $\mathrm{SL}_2(\mathbf{Z})$:

$$\begin{aligned} R &:= \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, & S &:= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, & T &:= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \\ U &:= \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, & V &:= TU^{-1} = \begin{pmatrix} -1 & 1 \\ -2 & 1 \end{pmatrix}. \end{aligned}$$

Before classifying the imprimitive representations of index 3, we describe the subgroups of Γ of index 3. This is well-known, but we give it for completeness.

Lemma 1. *The group Γ contains exactly four subgroups of index 3. One of these is normal, and it is a congruence subgroup of level 3. The remaining three subgroups are conjugate to $\bar{\Gamma}_0(2)$.*

Proof. Let $G \subseteq \Gamma$ be of index 3. Left multiplication of Γ on cosets of G defines a morphism of groups $\varphi : \Gamma \rightarrow S_3$ and the image has order 3 or 6. Let $K := \ker \varphi$. Then $K \subseteq G$, and either $\ker \varphi = G$, or else $\mathrm{im} \varphi \cong S_3$. In the first case $G \trianglelefteq \Gamma$, so $\Gamma/G \cong \mathbf{Z}_3$ and thus $\bar{T}^3 \in G$. But $\bar{\Gamma}(3)$ is the normal closure of \bar{T}^3 in Γ , so G contains $\bar{\Gamma}(3)$.

In the second case $\Gamma/K \cong S_3$ and G/K is a subgroup of order 2. Now the image of \bar{T} in Γ/K has order 2 or 3, and if it is 3 then as before $K \supseteq \bar{\Gamma}(3)$. However, $\bar{\Gamma}/\bar{\Gamma}(3) \cong A_4$, and this group does not have S_3 as a homomorphic image. This shows that \bar{T} has order 2, so K contains the normal closure of \bar{T}^2 , which is $\bar{\Gamma}(2)$. Because both K and $\bar{\Gamma}(2)$ both have index 6 in Γ , we deduce that $K = \bar{\Gamma}(2)$. By Sylow's theorem, G/K is conjugate to $\langle \bar{T} \rangle K/K = \bar{\Gamma}_0(2)/K$, so G is conjugate to $\bar{\Gamma}_0(2)$. \square

Inducing one-dimensional representations from the normal subgroup of Γ of index 3 gives rise to congruence modular forms, and so we will ignore these representations

in what follows. The representations of Γ obtained from inducing characters of a non-normal subgroup G of index three are (up to isomorphism) independent of the choice of G because (Lemma 1) all such G are conjugate. We thus focus on those representations induced from $\bar{\Gamma}_0(2)$.

Note that $\bar{V} \in \bar{\Gamma}_0(2)$ has order 2. It is well-known that $\bar{\Gamma}(2) = \langle \bar{T}^2, \bar{U} \rangle$ is a free group of rank 2. Then $\bar{\Gamma}_0(2) = \langle \bar{T}, \bar{U} \rangle = \langle \bar{T}^2, \bar{U} \rangle \rtimes \langle \bar{V} \rangle$, and we have the relation

$$\bar{T}\bar{U}\bar{T}^{-1}\bar{U}^{-1} = \bar{T}^2\bar{U}^2.$$

We assert that $N := \bar{\Gamma}(2)' \langle \bar{T}^2\bar{U}^2 \rangle = \bar{\Gamma}_0(2)'$. That $N \subseteq \bar{\Gamma}_0(2)'$ follows from the displayed relation. Observe that $N \trianglelefteq \bar{\Gamma}(2)$. Moreover $\bar{V}^{-1}\bar{T}^2\bar{V} = \bar{U}\bar{T}^2\bar{U}^{-1} \equiv \bar{T}^2 \pmod{N}$, and similarly (because \bar{V} is an involution) $\bar{V}^{-1}\bar{U}^2\bar{V} = \bar{T}\bar{U}^2\bar{T}^{-1} = (\bar{T}\bar{U}\bar{T}^{-1})^2 = (\bar{T}^2\bar{U}^3)^2 \equiv \bar{U}^2 \pmod{N}$. These calculations show not only that $N \trianglelefteq \bar{\Gamma}_0(2)$, but also that the quotient $\bar{\Gamma}_0(2)/N$ is abelian. The equality $N = \bar{\Gamma}_0(2)'$ then follows.

From the identification of $\bar{\Gamma}_0(2)$, it is immediate that $\bar{\Gamma}_0(2)/\bar{\Gamma}_0(2)' \cong \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})$, and that we can take the two summands to be generated by (the images of) \bar{U} and \bar{V} respectively.

Now suppose that $\chi : \bar{\Gamma}_0(2) \rightarrow \mathbf{C}^\times$ is a character of finite order. Since χ factors through the abelianization of $\bar{\Gamma}_0(2)$, it follows from the preceding discussion that there exists a primitive n th root of unity λ and a sign $\varepsilon = \pm 1$ such that

$$(2) \quad \chi(\bar{U}) = \lambda, \quad \chi(\bar{V}) = \varepsilon.$$

We now consider the induced representation

$$\rho := \text{Ind}_{\bar{\Gamma}_0(2)}^{\Gamma} \chi.$$

Essentially by definition, the underlying module V furnishing ρ is a direct sum

$$V = V_0 \oplus V_1 \oplus V_2$$

of 1-dimensional vector spaces V_j , where V_0 affords χ and the V_j are permuted transitively by Γ . We fix this notation for the remainder of this section.

Proposition 2. *With respect to an ordered basis v_0, v_1, v_2 of V with $v_j \in V_j$, and up to a possible reordering of V_1 and V_2 , we have*

$$\rho(\bar{R}) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \rho(\bar{S}) = \varepsilon \begin{pmatrix} 0 & 0 & \lambda \\ 0 & 1 & 0 \\ \bar{\lambda} & 0 & 0 \end{pmatrix}, \quad \rho(\bar{T}) = \varepsilon \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 0 & 1 \\ 0 & \bar{\lambda} & 0 \end{pmatrix}.$$

In particular, the eigenvalues of $\rho(\bar{T})$ are $\{\varepsilon\lambda, \pm\sigma\}$ for some σ such that $\sigma^2 = \bar{\lambda}$.

Proof. Since Γ permutes the V_j transitively and the stabilizer of V_0 is $\bar{\Gamma}_0(2)$, then $\bar{\Gamma}(2)$ leaves each V_j invariant and the quotient $\bar{\Gamma}/\bar{\Gamma}_0(2) \cong S_3$ induces every possible permutation of the V_j .

Since \bar{R} has order 3 we may choose notation so that $\rho(\bar{R}) : v_2 \mapsto v_1 \mapsto v_0 \mapsto v_2$, where v_j spans V_j . Then with respect to the ordered basis v_0, v_1, v_2 , $\rho(\bar{R})$ is as indicated. Now $\rho(\bar{T}) = \rho(\bar{V})\rho(\bar{U})$ has v_0 as eigenvector with eigenvalue $\varepsilon\lambda$. Moreover, $\rho(\bar{T})$ and interchanges V_1 and V_2 . Therefore, we have

$$\rho(\bar{T}) = \begin{pmatrix} \varepsilon\lambda & 0 & 0 \\ 0 & 0 & u \\ 0 & v & 0 \end{pmatrix}$$

for scalars u, v . We assert that $uv = \bar{\lambda}$. To see this, use the relation $\bar{R}\bar{T}^2\bar{R}^{-1} = \bar{U}^{-1}$ to obtain

$$\bar{T}^2V_1 = \bar{T}^2\bar{R}^{-1}V_0 = \bar{R}^{-1}\bar{U}^{-1}V_0 = \bar{\lambda}V_1.$$

This says that the eigenvalue of $\rho(\bar{T}^2)$ on V_1 is $\bar{\lambda}$, and our assertion follows. Since $\bar{S}\bar{R} = \bar{T}$, we find that

$$\rho(\bar{S}) = \rho(\bar{T})\rho(\bar{R})^{-1} = \begin{pmatrix} \varepsilon\lambda & 0 & 0 \\ 0 & 0 & u \\ 0 & v & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & \varepsilon\lambda \\ 0 & u & 0 \\ v & 0 & 0 \end{pmatrix},$$

so that

$$\rho(\bar{S}^2) = \begin{pmatrix} \varepsilon v\lambda & 0 & 0 \\ 0 & u^2 & 0 \\ 0 & 0 & \varepsilon v\lambda \end{pmatrix} = I.$$

Since $uv = \bar{\lambda}$, we see that $u = \varepsilon$, and the matrices representing \bar{T} and \bar{S} are then as in the statement of the Proposition. \square

Lemma 3. *There is a short exact sequence*

$$1 \rightarrow A \rightarrow \rho(\bar{\Gamma}) \rightarrow S_3 \rightarrow 1,$$

where $A := \rho(\bar{\Gamma}(2)) = \langle \rho(\bar{T}^2), \rho(\bar{U}) \rangle$, and exactly one of the following holds:

- (i) $\gcd(n, 3) = 1$ and $A \cong \mathbf{Z}_n \times \mathbf{Z}_n$;
- (ii) $3|n$ and $A \cong \mathbf{Z}_n \times \mathbf{Z}_{n/3}$.

Proof. From Lemma 2 we obtain

$$\rho(\bar{T}^2) = \begin{pmatrix} \lambda^2 & 0 & 0 \\ 0 & \bar{\lambda} & 0 \\ 0 & 0 & \bar{\lambda} \end{pmatrix}, \quad \rho(\bar{U}) = \rho(\bar{R}\bar{T}^{-2}\bar{R}^{-1}) = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \bar{\lambda}^2 \end{pmatrix}.$$

Now all parts of the Lemma can be checked directly. \square

Lemma 4. *The following statements are equivalent:*

- (i) $n|3$,
- (ii) ρ is not irreducible,
- (iii) $\rho(\bar{T})$ has repeated eigenvalues.

Proof. By Lemma 2, $\rho(\bar{T})$ has a repeated eigenvalue if, and only if, $\varepsilon\lambda = \pm\sigma$. Because $\sigma^2 = \bar{\lambda}$ (cf. Lemma 2) this is equivalent to $\lambda^3 = 1$, so (i) and (iii) are equivalent.

Now we show that (ii) and (iii) are also equivalent. If ρ is not irreducible then its complete reducibility (which holds because $\rho(\Gamma)$ is finite) means that $\rho(\Gamma)$ leaves invariant some 1-dimensional subspace of V . If $\rho(\bar{T})$ has distinct eigenvalues then such an invariant subspace is necessarily one of the 3 eigenspaces for $\rho(\bar{T})$. These are spanned by

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \\ \sigma \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \\ -\sigma \end{pmatrix},$$

where $\sigma^2 = \bar{\lambda}$. However, from the explicit nature of the matrix $\rho(\bar{S})$ given in Proposition 2, we see that none of these three eigenspaces are invariant under $\rho(\bar{S})$, and this is a contradiction. Thus we have established the implication (ii) \Rightarrow (iii).

Conversely, if (iii) holds then we know that $\lambda^3 = 1$. Then we check directly that $\rho(\bar{S})$ and $\rho(\bar{T})$ each leave the span of $\begin{pmatrix} 1 \\ \lambda \\ \lambda^2 \end{pmatrix}$ invariant, in which case (ii) holds. This completes the proof of the Lemma. \square

Our next theorem determines when ρ factors through a congruence quotient of Γ . This will be important for recognizing when vvmfs are themselves congruence.

Theorem 5. *Let ρ be a representation of Γ that is induced from a one-dimensional representation χ of $\bar{\Gamma}_0(2)$ with finite image. Let n be such that $\chi(\bar{U})$ is a primitive n th root of unity. Then $\ker \rho$ is a congruence subgroup if, and only if, $n|24$.*

Proof. In the following proof, we repeatedly use the fact that if $G \subseteq \Gamma$ is a congruence subgroup, then for a positive integer N , $\bar{\Gamma}(N) \subseteq G$ if, and only if, $\bar{T}^N \in G$.

Set $K := \ker \rho$. We assume until further notice that K is a congruence subgroup. From Lemma 2 it follows that $\rho(\bar{T})$ has order $2n$. Thus $\bar{T}^{2n} \in K$, and because K is assumed to be congruence then $\bar{\Gamma}(2n) \subseteq K$, and K has level *exactly* $2n$. If n is divisible by a prime $p \geq 5$, it follows that $\Gamma/\bar{\Gamma}(2n)$ has a quotient $\Gamma/\bar{\Gamma}(p) \cong \text{PSL}_2(p)$, which is nonsolvable. On the other hand, this same group must also be a quotient of $\rho(\Gamma)$, which is solvable by Lemma 3, contradiction. So n is divisible only by the primes 2 and 3.

Suppose next that $16|n$. We shall derive a contradiction. Let M be the unique normal subgroup of $\bar{\Gamma}(2)$ such that $\bar{\Gamma}(2)/M \cong \mathbf{Z}_{16}^2$. From the description of A in Lemma 3 we see that $K \subseteq M$. As K is congruence and $\bar{T}^{32} \in M$, we have $\bar{\Gamma}(32) \subseteq M$. In effect, this reduces us to deriving a contradiction if $n = 16$ and $K = M$. Indeed, consider the tower of groups

$$N := \bar{\Gamma}(2) \supseteq \bar{\Gamma}(4) \supseteq \bar{\Gamma}(8) \supseteq \bar{\Gamma}(16) \supseteq \bar{\Gamma}(32) =: N_1$$

Note that $N/\bar{\Gamma}(4) \cong \mathbf{Z}_2^2$ and the other quotients satisfy $\bar{\Gamma}(2^f)/\bar{\Gamma}(2^{f+1}) \cong \mathbf{Z}_2^3$. The element \bar{R} acts on each of these latter quotients by conjugation, with fixed-point subgroup of order 2. So we have $|N/N_1| = 2^{11}$ and $|C_{N/N_1}(\bar{R})| = 2^3$. On the other hand, \bar{R} acts without fixed-points on N/M , and $N_1 \subseteq M$. We conclude that $K/N_1 = C_{N/N_1}(\bar{R}) \trianglelefteq N/N_1$ where $C_{N/N_1}(\bar{R})$ denotes the fixed points of \bar{R} acting on N/N_1 . However, one can calculate explicitly that this is *false*, and this is the desired contradiction.

Assume that $9|n$. By Lemma 3 we can find a subgroup M such that $K \subseteq M \subseteq \bar{\Gamma}(2)$ and $\bar{\Gamma}(2)/M \cong \mathbf{Z}_3^2$. Then $\bar{T}^6 \in M$, whence also $M \supseteq \bar{\Gamma}(6)$. But then $\bar{\Gamma}(2)/M$ is a quotient of $\bar{\Gamma}(2)/\bar{\Gamma}(6)$ of order 9, a contradiction because $|\bar{\Gamma}(2)/\bar{\Gamma}(6)| = 12$. This completes the proof of the statement K congruence $\Rightarrow n|24$. It remains to prove the converse.

Writing K_n to indicate the dependence of K on n , it follows from Lemma 3 that $K_n \subseteq K_m$ if $m|n$. Therefore, it suffices to assume that $n = 24$ and show that $K = K_{24}$ is congruence. We will actually show that

$$(3) \quad K_{24} = \bar{\Gamma}(2)' \bar{\Gamma}(48).$$

By Lemma 3 we have $\bar{\Gamma}(2)/K_{24} \cong \mathbf{Z}_{24} \times \mathbf{Z}_8$, and in particular, there is a *unique* subgroup M satisfying $K \subseteq M \subseteq \bar{\Gamma}(2)$ and $|\bar{\Gamma}(2)/M| = 3$. The unicity of M ensures that $M \trianglelefteq \Gamma$, and one readily deduces that $\bar{\Gamma}(6) \subseteq M$. Since $\bar{\Gamma}(2)/\bar{\Gamma}(6) \cong \text{PSL}_2(3) \cong A_4$, then $M/\bar{\Gamma}(6) = (\bar{\Gamma}(2)/\bar{\Gamma}(6))'$, i.e., $M = \bar{\Gamma}(6)\bar{\Gamma}(2)'$.

Since $M/\bar{\Gamma}(2)'$ is a free abelian group of rank 2 then $K/\bar{\Gamma}(2)'$ is the *unique* subgroup with quotient $\mathbf{Z}_8 \times \mathbf{Z}_8$. Now $\bar{\Gamma}(48)\bar{\Gamma}(2)' \subseteq \bar{\Gamma}(6)\bar{\Gamma}(2)' \subseteq M$, so if we can also show that $M/\bar{\Gamma}(48)\bar{\Gamma}(2)' \cong \mathbf{Z}_8 \times \mathbf{Z}_8$, then (3) will follow. From the last paragraph, this is the same as showing that $\bar{\Gamma}(6)\bar{\Gamma}(2)'/\bar{\Gamma}(48)\bar{\Gamma}(2)' \cong \mathbf{Z}_8 \times \mathbf{Z}_8$.

We interpolate a general Lemma.

Lemma 6. *Suppose that A, B, C are normal subgroups of a group G with $B \subseteq A$. There is a commuting diagram*

$$\begin{array}{ccccccc} 1 & \longrightarrow & \frac{(B \cap C)(C \cap A')}{B \cap C} & \longrightarrow & \frac{A \cap C}{B \cap C} & \longrightarrow & \frac{(A \cap C)A'}{(B \cap C)A'} \longrightarrow 1 \\ & & \downarrow f_1 & & \downarrow f_2 & & \\ 1 & \longrightarrow & \frac{BA'}{B} & \longrightarrow & \frac{A}{B} & \longrightarrow & \frac{A}{BA'} \longrightarrow 1 \end{array}$$

where the horizontal rows are short exact, f_2 is injective, and the restriction f_1 of f_2 to the indicated subgroup is also injective. In particular, if f_2 is an isomorphism it induces an isomorphism of short exact sequences, and especially an isomorphism

$$(4) \quad \frac{(A \cap C)A'}{(B \cap C)A'} \cong \frac{A}{BA'}.$$

Proof. The lower short exact sequence is canonical. As for the upper sequence, the map $a(B \cap C) \mapsto a(B \cap C)A'$ ($a \in A \cap C$) induces a surjective morphism of groups $(A \cap C)/(B \cap C) \rightarrow (A \cap C)A'/(B \cap C)A'$ with kernel $(A \cap C) \cap (B \cap C)A'/(B \cap C) = (B \cap C)(A \cap C \cap A')/(B \cap C) = (B \cap C)(C \cap A')/(B \cap C)$, so that the upper sequence is also short exact.

Next, the map $a \mapsto aB$ ($a \in A \cap C$) induces a group morphism $A \cap C \rightarrow A/B$ with kernel $A \cap C \cap B = B \cap C$. Thus the middle vertical arrow f_2 , defined by $f_2(a(B \cap C)) = aB$, is injective, and we easily check that f_1 , which is the restriction of f_2 to $(B \cap C)(C \cap A')/(B \cap C)$, is also injective.

It is clear that the diagram commutes, so suppose now that f_2 is an isomorphism. Since $BA'/B = (A/B)'$ and $(A \cap C)A'/(B \cap C)A'$ is *abelian* then f_1 is necessarily *surjective*. Since it is also injective it is therefore an isomorphism, and the final assertions of the Lemma follow immediately. \square

We apply the Lemma with A, B, C equal to $\bar{\Gamma}(2), \bar{\Gamma}(16), \bar{\Gamma}(3)$ respectively. Because $A \cap C = \bar{\Gamma}(6)$ and $B \cap C = \bar{\Gamma}(48)$, (4) then reads

$$\frac{\bar{\Gamma}(6)\bar{\Gamma}(2)'}{\bar{\Gamma}(48)\bar{\Gamma}(2)'} \cong \frac{\bar{\Gamma}(2)}{\bar{\Gamma}(16)\bar{\Gamma}(2)'}$$

In order to complete the proof of the Theorem, it is therefore sufficient show that $\bar{\Gamma}(2)/\bar{\Gamma}(16)\bar{\Gamma}(2)' \cong \mathbf{Z}_8 \times \mathbf{Z}_8$. (In effect, we have reduced the proof to the case $n = 8$.)

Let $G := \bar{\Gamma}(2)/\bar{\Gamma}(16) = \langle \bar{T}^2\bar{\Gamma}(16), \bar{U}\bar{\Gamma}(16) \rangle$. We have $|G| = 2^8$. We calculate that

$$C := [T^2, U] = \begin{pmatrix} 21 & -8 \\ 8 & -3 \end{pmatrix},$$

that the image of \bar{C} in G has order 4, and that $[C, T^2] \equiv [C, U] \equiv I \pmod{16}$. Thus $\langle \bar{C}\bar{\Gamma}(16) \rangle = G'$ has order 4, so that $G/G' \cong \bar{\Gamma}(2)/\bar{\Gamma}(2)'\bar{\Gamma}(16)$ is abelian with 2 generators, exponent 8 and order 2^6 . Therefore $\bar{\Gamma}(2)/\bar{\Gamma}(2)'\bar{\Gamma}(16) \cong \mathbf{Z}_8 \times \mathbf{Z}_8$, and the proof of Theorem 5 is complete. \square

3. GEOMETRIC CONSIDERATIONS

We retain previous notation, in particular, $\chi: \bar{\Gamma}_0(2) \rightarrow \mathbf{C}^\times$ is the linear character described in (2), and we put $\rho = \text{Ind}_{\bar{\Gamma}_0(2)}^\Gamma \chi$, $K = \ker \rho$ and $A = \bar{\Gamma}(2)/K$. We also set

$$H := \ker \chi, \quad H_0 := H \cap \bar{\Gamma}(2), \quad H_1 := H_0 \langle \bar{V} \rangle, \quad H_2 := H \langle \bar{V} \rangle.$$

We collectively refer to these groups as the H -groups. Note that the group H , and thus all of the H -groups, does not depend on the particular primitive n th root of unity $\lambda = \chi(\bar{U})$, it only depends on its order n and the sign ε satisfying $\chi(\bar{V}) = \varepsilon$. The next fact is only slightly less obvious.

Lemma 7. *The group H_0 depends only on the order n of $\chi(\bar{U})$.*

Proof. Note that $\ker \chi$ is generated by \bar{U}^n , $\bar{\Gamma}_0(2)'$, and \bar{V}^m where $m = 0$ or 1 . We thus wish to show that

$$\langle \bar{U}^n, \bar{V} \rangle \bar{\Gamma}_0(2)' \cap \bar{\Gamma}(2) = \langle \bar{U}^n \rangle \bar{\Gamma}_0(2)' \cap \bar{\Gamma}(2).$$

Now $\bar{U} \in \bar{\Gamma}(2)$, so the group on the right is just $\langle \bar{U}^n \rangle \bar{\Gamma}_0(2)'$. Similarly, the group on the left can be written as $\langle \bar{U}^n \rangle \bar{\Gamma}_0(2)' \langle \bar{V} \rangle \cap \bar{\Gamma}(2) = \langle \bar{U}^n \rangle \bar{\Gamma}_0(2)' \langle (\bar{V}) \cap \bar{\Gamma}(2) \rangle = \langle \bar{U}^n \rangle \bar{\Gamma}_0(2)'$. This completes the proof of the Lemma. \square

We are interested in the algebraic curves defined by the H -groups. In order to study these objects, we require more group-theoretic data about the H -groups themselves. Notice that $\bar{\Gamma}_0(2)' \subseteq H_0$. Thus the H -groups are each *normal* in $\bar{\Gamma}_0(2)$ with abelian quotient. Their precise relation to each other depends on ε and the parity of n , and we explain this first.

Lemma 8. *One of the following holds:*

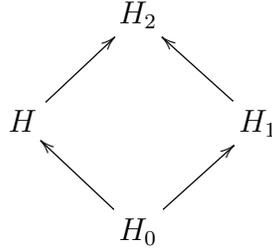
- A. n is odd, $\varepsilon = -1$, $H = H_0$ and $H_1 = H_2$;
- B. n is odd, $\varepsilon = +1$ and $H = H_1 = H_2$;
- C. n is even, $\varepsilon = -1$, all four of the H -groups are distinct and $|H_2/H_0| = 4$;
- D. n is even, $\varepsilon = +1$ and $H = H_1 = H_2$.

Moreover, in all cases $|H_1/H_0| = 2$.

Proof. Because $\bar{V} \in \bar{\Gamma}_0(2) \setminus \bar{\Gamma}(2)$ we always have $|H_1/H_0| = 2$. If $\varepsilon = +1$ then $\chi(\bar{V}) = 1$, so $\bar{V} \in H \setminus H_0$ and B or D holds according to the parity of n .

If n is odd and $\varepsilon = -1$ then from (2) we see immediately that $\ker \chi \subseteq \bar{\Gamma}(2)$, i.e., $H = H_0$. Then A holds.

Finally, if n is even and $\varepsilon = -1$ then we again use (2) to see that $\ker \chi$ contains an element in $\bar{\Gamma}_0(2) \setminus \bar{\Gamma}(2)$, whereas $\bar{V} \notin \ker \chi$. Pictorially, there is a diagram of containments of index 2:



This is case C. □

In what follows, we refer to the different possibilities of the preceding Lemma as Case A, Case B, etc.

Lemma 9. *The following hold.*

- (i) $|\bar{\Gamma}(2)/H_0| = |\bar{\Gamma}_0(2)/H_1| = n$.
- (ii) $\bar{\Gamma}(2) = H_0\langle\bar{U}\rangle = H_0\langle\bar{T}\bar{U}\bar{T}^{-1}\rangle$.
- (iii) $|\bar{\Gamma}(2)/H_0\langle\bar{T}^2\rangle| \leq 2$ with equality if and only if n is even.

Proof. Since the abelianization of $\bar{\Gamma}_0(2)$ is generated by the images of \bar{V}, \bar{U} and $\bar{V} \notin \bar{\Gamma}(2)$, it follows that $\bar{\Gamma}(2) = H_0\langle\bar{U}\rangle$. Then because $\chi(\bar{U}) = \lambda$ is a primitive n th root of unity, the first equality of part (i) of the Lemma follows immediately. The second follows because $|H_1/H_0| = 2$ (Lemma 8).

We have already established the first equality in part (ii). Then because \bar{V} normalizes both $\bar{\Gamma}(2)$ and H_0 , and since $\bar{V}\bar{U}\bar{V}^{-1} = \bar{T}\bar{U}\bar{T}^{-1}$, the second equality also holds.

Finally, the equality $\chi(\bar{T}^2) = \lambda^2$ follows from Lemma 2. Part (iii) is an immediate consequence of this together with part (i). This completes the proof of the Lemma. □

Lemma 10. *The group $\bar{\Gamma}_0(2)$ contains a unique conjugacy class of involutions, and H_1 contains n conjugacy classes of involutions. In Case C, H_2 contains $n/2$ conjugacy classes of involutions.*

Proof. It is well-known that $\bar{\Gamma}_0(2)$ has a unique conjugacy class of involutions, but here's a proof: it is even more well-known that Γ has a unique such conjugacy class. So if $x, y \in \bar{\Gamma}_0(2)$ are two involutions, there is $g \in \Gamma$ such that $g^{-1}xg = y$. Since $\bar{\Gamma}_0(2) = \bar{\Gamma}(2)\langle x \rangle = \bar{\Gamma}(2)\langle y \rangle$, it follows that g normalizes $\bar{\Gamma}_0(2)$. But this latter group is self-normalizing (cf. Lemma 1), whence $g \in \bar{\Gamma}_0(2)$. Thus x and y are conjugate in $\bar{\Gamma}_0(2)$ and the proof is complete.

Now $\bar{V} \in H_1 \trianglelefteq \bar{\Gamma}_0(2)$. Since \bar{V} is an involution, all involutions of $\bar{\Gamma}_0(2)$ are contained in H_1 by the first paragraph. Involutions of $\bar{\Gamma}$ being self-centralizing, it follows that the conjugation action of H_1 on its involutions falls into $|\bar{\Gamma}_0(2)/H_1|$ classes that are themselves transitively permuted by $\bar{\Gamma}_0(2)$. Since $|\bar{\Gamma}_0(2)/H_1| = n$ by Lemma 9 then H_1 has n classes of involutions.

In Case C, the identical proof applies with H_2 in place of H_1 . The only difference is that H_2 has index $n/2$ in $\bar{\Gamma}_0(2)$, so that it has $n/2$ classes of involutions. This completes the proof of the Lemma. □

Lemma 11. *In cases A, B and D we have $\bar{\Gamma}_0(2)/H_1 = \{\bar{U}^j H_1, 0 \leq j \leq n-1\}$. Representatives for the elliptic points of H_1 are the numbers*

$$\{U^{-j}(1+i)/2 \mid 0 \leq j \leq n-1\} = \left\{ \frac{1}{-2j+(1-i)} \mid 0 \leq j \leq n-1 \right\}.$$

Proof. By Lemma 9 we have $|\bar{\Gamma}_0(2)/H_1| = n$. Now each $\bar{U}^j \in \bar{\Gamma}_0(2)$, and since $\chi(\bar{U}^j) = \lambda^j \neq 1$ for $0 \leq j \leq n-1$ then these elements give *distinct* representatives of $\bar{\Gamma}_0(2)/H_1$. So if $H = H_1$ we are done. This handles cases B and D by Lemma 8. In case A, we have $H_1 = H\langle \bar{V} \rangle$, and if some $\bar{U}^j \in H\bar{V}$ then $\lambda^j = \chi(\bar{U}^j) = \chi(\bar{V}) = -1$, and this is impossible because n is *odd* in case A. This completes the proof of the first assertion of the Lemma in all three cases.

It follows from this and the discussion presented in the course of the proof of Lemma 10, that the n conjugacy classes of involutions in H_1 have representatives $\bar{U}^{-j}\bar{V}\bar{U}^j$ ($0 \leq j \leq n-1$). Since \bar{V} itself has fixed-point $\frac{1+i}{2}$, it follows that the elliptic points of H_1 are represented by $\bar{U}^{-j}(\frac{1+i}{2})$, and the Lemma is proved. \square

Now we are ready to study the curves. If $B \subseteq \Gamma$ is a subgroup of finite index, we write X_B for the projective algebraic curve whose complex points are identified with $B \backslash \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$. In the special cases $B = \bar{\Gamma}(N)$ or $\bar{\Gamma}_0(2)$, we denote the corresponding curves by $X(N)$ and $X_0(N)$, respectively. The *genus* of X_B is denoted by g_B .

Containments among the H -groups define various natural coverings of degree 2 among the corresponding curves (cf. Lemma 8):

$$X_{H_0} \rightarrow X_{H_1} \quad (\text{Cases A, B, D})$$

and

$$(5) \quad \begin{array}{ccc} & X_{H_0} & \\ & \swarrow \quad \searrow & \\ X_H & & X_{H_1} \\ & \searrow \quad \swarrow & \\ & X_{H_2} & \end{array} \quad (\text{Case C})$$

We can now state the first main result of this Section.

Theorem 12. *The curve X_{H_1} has two cusps $\{\infty, 0\}$ and genus 0. In particular, X_{H_0} is a hyperelliptic curve.*

To prove this we must translate the group-theoretic facts about the H -groups established earlier into geometric facts about the corresponding algebraic curves.

Lemma 13. *If n is odd, X_{H_0} has three cusps $\{\infty, 0, 1\}$ and genus $(n-1)/2$.*

Proof. Recall that $\bar{\Gamma}(2)$ has three cusps, with representatives given by $\infty, 0$ and 1 . These cusps are stabilized by \bar{T}, \bar{U} and $\bar{T}\bar{U}\bar{T}^{-1}$ respectively, and because we are assuming that n is odd, Lemma 9(ii), (iii) makes it clear that H_0 has the *same* three cusps as $\bar{\Gamma}(2)$.

Because $\bar{\Gamma}(2)$ is free, the covering $X_{H_0} \rightarrow X(2)$ is regular of degree n away from the cusps, and fully ramified at the cusps. By the Riemann-Hurwitz theorem, we see that the genus of H_0 is $(n-1)/2$, as claimed. \square

Similarly, we have

Lemma 14. *If n is even, X_{H_0} has four cusps $\{0, 1, 1/2, \infty\}$ and genus $(n-2)/2$.*

Proof. The points 0 and 1 are distinct cusps of H_0 by the same proof as before (using Lemma 9(ii)). Part (iii) of the same Lemma shows that when n is even, ∞ behaves slightly differently, because now $\bar{\Gamma}(2) = H_0\langle\bar{T}^2\rangle \cup H_0\langle\bar{T}^2\rangle\bar{U}$, so that

$$\bar{\Gamma}(2) \cdot \infty = (H_0\langle\bar{T}^2\rangle \cup H_0\langle\bar{T}^2\rangle\bar{U}) \cdot \infty = H_0 \cdot \infty \cup H_0 \cdot \frac{1}{2}.$$

This shows that H_0 has four cusps $\{0, 1, 1/2, \infty\}$. Moreover, in the covering $X_{H_0} \rightarrow X(2)$, the cusps 0 and 1 are fully ramified and the ramification index at the other two cusps is $n/2$. The Riemann-Hurwitz theorem again implies the desired genus formula. \square

We turn to the proof of Theorem 12. The relevant picture is as follows:

$$(6) \quad \begin{array}{ccc} X_{H_0} & & \\ \downarrow 2 & \searrow n & \\ & & X(2) \\ & & \downarrow 2 \\ X_{H_1} & \searrow n & \\ & & X_0(2) \end{array}$$

where the arrow labels denote degrees of maps (cf. Lemma 9). We will apply the Riemann-Hurwitz formula to the left vertical covering. The details are slightly different according to the parity of n , so let us first assume that n is odd. Then by Lemma 13, H_0 has cusps $\{\infty, 0, 1\}$ and genus $(n-1)/2$. As $H_1 = H_0\langle\bar{V}\rangle$ and \bar{V} exchanges the cusps $\{0, 1\}$, X_{H_1} has two cusps and only the infinite cusp of X_{H_0} ramifies. The n elliptic points of H_1 (enumerated in Lemma 11) as well as ∞ , each make a contribution of 1 to $\sum_P(e_P - 1)$, where e_P is the ramification degree at a point $P \in X_{H_0}$. Therefore,

$$2 - 2g_{H_0} = 2(2 - g_{H_1}) - \sum_P(e_P - 1) \Rightarrow 3 - n = 4 - 2g_{H_1} - (n + 1),$$

and the desired result $g_{H_1} = 0$ follows.

Now suppose that n is even. By Lemma 14, H_0 has cusps $\{\infty, 0, 1, 1/2\}$ and genus $(n-2)/2$. In this case, we can check directly that \bar{V} exchanges the cusps $\{0, 1\}$ and $\{\infty, 1/2\}$. So the only ramification arises from the n elliptic points of X_{H_1} (Lemma 10 still applies), and we now obtain

$$4 - n = 4 - 2g_{H_1} - n,$$

leading once again to $g_{H_1} = 0$. This completes the proof of the Theorem. \square

A similar argument shows

Theorem 15. *In Case C, X_H is a hyperelliptic curve of genus $[n/4]$.*

Proof. (Sketch). Refer to (5) for the picture in this case. Since X_{H_1} has genus 0 by Theorem 12, the same is true of X_{H_2} . Therefore, X_H is hyperelliptic. X_{H_0} has 4 cusps $\{\infty, 0, 1, 1/2\}$, $H = H_0\langle \bar{U}^{n/2}\bar{V} \rangle$, and $\bar{U}^{n/2}\bar{V}$ exchanges the cusps $\{0, 1\}$. H contains no involutions, hence it is free, so the only ramification in the covering $X_{H_0} \rightarrow X_H$ occurs at the cusps, and there are $f := 0$ or 2 ramified cusps. Now Riemann-Hurwitz yields

$$4 - n = 2(2 - 2g_H) - f \Rightarrow g_H = (n - f)/4 = [n/4].$$

□

We end this section by describing algebraic equations for the hyperelliptic curves discussed in Theorem 12. Let $\rho = \text{Ind}_{\Gamma_0(2)}^{\Gamma} \chi$ be a representation as above, and assume that we are in Case A, B or D of Lemma 8. The diagram (6) applies, and the discussion of the previous section tells us that the curve $X_0(2)$ has two cusps $\{0, \infty\}$ and similarly for X_{H_1} . The bottom map in (6) is ramified only at the cusps, and it is of degree n . Both are curves of genus 0. A hauptmodul for $\Gamma_0(2)$ is given by

$$K_0(\tau) = \frac{\eta(\tau)^{24}}{\eta(2\tau)^{24}},$$

and one can use the transformation properties of the Dedekind eta function η , and the factorization formula for η , to verify that $K_0(0) = 0$ and $K_0(\infty) = \infty$. It follows that $\sqrt[n]{K_0}$ is a hauptmodul for H_1 .¹

In order to find an algebraic equation for the hyperelliptic curve X_{H_0} we must understand the ramification of the projection map $X_{H_0} \rightarrow X_{H_1}$ of degree two. If n is odd then this map is ramified at the cusp ∞ and at the elliptic points of H_1 , while if n is even then this map is only ramified at the elliptic points. We have seen that the set of elliptic points is equal to the following set:

$$\left\{ U^{-j} \left(\frac{1+i}{2} \right) \mid 0 \leq j \leq n-1 \right\}.$$

Since K_0 is invariant under Γ , it takes the same value on all of these elliptic points. Further, since the powers of \bar{U} give a set of coset representatives for $H_1 \backslash \bar{\Gamma}_0(2)$, it follows that the values $\sqrt[n]{K_0}(U^{-j}(1+i)/2)$ are the n distinct n th roots of $K_0((1+i)/2)$ and $y^2 = x^n - K_0((1+i)/2)$ is an affine algebraic equation for the hyperelliptic curve $X_{H_0} \rightarrow X_{H_1}$. By the theory of complex multiplication, one knows that $K_0((1+i)/2)$ is a rational number. In fact, one can use the Chowla-Selberg formula to show that $K_0((1+i)/2) = -64$. This shows that in cases A, B and D, the curve X_{H_0} can be described by the affine hyperelliptic equation $y^2 = x^n + 64$. We summarize some of our conclusions in

Theorem 16. *Assume that one of Cases A, B or D of Lemma 8 holds. Then X_{H_1} has genus 0, and the double cover $X_{H_0} \rightarrow X_{H_1}$ has genus $[\frac{n-1}{2}]$ and is described by the affine hyperelliptic equation $y^2 = x^n + 64$.* □

¹Compare this result with Theorem 5.

Remark 17. Ultimately we will only prove ASD-style congruences for modular forms arising in Case A, so we have not determined what hyperelliptic curves arise in Theorem 15.

4. VECTOR-VALUED MODULAR FORMS OF MINIMAL WEIGHT

Section 4.3 of [6] explains how generalized hypergeometric series and the free-module theorem of [15] allow one to describe the module of vector-valued modular forms associated to an irreducible three-dimensional representation of Γ . The answer is expressed in terms of the exponents of the eigenvalues of $\rho(\bar{T})$.

Let $\rho = \text{Ind}_{\Gamma_0(2)}^{\bar{\Gamma}} \chi$ be as in Theorem 2, and write $\chi(\bar{U}) = e^{2\pi ir/n} = \lambda$ where $0 < r < n$ and $\text{gcd}(r, n) = 1$. Let ρ' be a representation of Γ equivalent with ρ such that

$$\rho'(\bar{T}) = \text{diag}(\varepsilon\lambda, \sigma, -\sigma),$$

where $\sigma^2 = \bar{\lambda}$. Define $\mathbf{e}(z) = e^{2\pi iz}$. Then we have the following cases:

$$\rho'(\bar{T}) = \begin{cases} \mathbf{e}(\text{diag}(\frac{2r+n}{2n}, \frac{n-r}{2n}, \frac{2n-r}{2n})) & \text{Cases A and C,} \\ \mathbf{e}(\text{diag}(\frac{2r}{2n}, \frac{n-r}{2n}, \frac{2n-r}{2n})) & \text{Cases B and D.} \end{cases}$$

Not all of the exponents above necessarily lie between 0 and 1. Since we've chosen r to satisfy $0 < r < n$, it follows that r/n , $(n-r)/(2n)$ and $(2n-r)/(2n)$ all lie in $[0, 1)$. However, if $r \geq n/2$ then $(2r+n)/(2n)$ does not lie between 0 and 1. In this case we replace the exponent by $(2r-n)/2n$. If we let r_1 , r_2 and r_3 denote these normalized exponents, then it's known (e.g., Lemma 2.3 of [13]) that the minimal weight k_0 for ρ satisfies $k_0 = 4(r_1 + r_2 + r_3) - 2$. Note that in all cases, if r is chosen as above then $r_2 = (n-r)/(2n)$, $r_3 = (2n-r)/(2n)$, and the following table summarizes the possibilities for r_1 and k_0 :

	r_1	k_0
Cases A,C and $r \geq n/2$	$\frac{2r-n}{2n}$	2
Cases A,C and $r < n/2$	$\frac{2r+n}{2n}$	6
Cases B,D	$\frac{r}{n}$	4

The value of r_1 can be written uniformly as follows: set

$$e = \begin{cases} -1 & \text{in Cases A,C and } r \geq n/2, \\ 0 & \text{in Cases B,D,} \\ 1 & \text{in Cases A,C and } r < n/2. \end{cases}$$

then $r_1 = (2r + en)/(2n)$ and $k_0 = 2e + 4$. The exponent differences satisfy:

$$r_1 - r_2 = \frac{3r + (e-1)n}{2n}, \quad r_1 - r_3 = \frac{3r + (e-2)n}{2n}, \quad r_2 - r_3 = -\frac{1}{2}.$$

Thus, the only way that one of these differences can be an integer is if $n|3$. By Lemma 4 these are precisely the cases where ρ is reducible. Assume that $n \nmid 3$ and write

$$a = r_1 - \frac{k_0}{12}, \quad b = r_2 - \frac{k_0}{12}, \quad c = r_3 - \frac{k_0}{12}.$$

Then a basis (over the ring of classical scalar modular forms of level 1) for the module of vector-valued modular forms for ρ' is given by (F, DF, D^2F) , where $D = q \frac{d}{dq} - \frac{k}{12} E_2$

denotes the modular derivative of weight k , and where F is the vector-valued modular form

$$(7) \quad F = \eta^{2k_0} \begin{pmatrix} K^a {}_3F_2 \left(a, a + \frac{1}{3}, a + \frac{2}{3}; a - b + 1, a - c + 1; K \right) \\ K^b {}_3F_2 \left(b, b + \frac{1}{3}, b + \frac{2}{3}; b - a + 1, b - c + 1; K \right) \\ K^c {}_3F_2 \left(c, c + \frac{1}{3}, c + \frac{2}{3}; c - a + 1, c - b + 1; K \right) \end{pmatrix}.$$

Here $K = 1728j^{-1}$ and j denotes the usual j -invariant of elliptic curves. Our first result on F is the following.

Lemma 18. *The following are equivalent.*

- (i) At least one of the components of F is a modular form on a congruence subgroup,
- (ii) all of the components of F are modular forms on a congruence subgroup,
- (iii) $\ker \rho'$ is a congruence subgroup,
- (iv) $n|24$.

In particular, all components of F have bounded denominators if any of these conditions holds.

Proof. Since ρ and ρ' are equivalent representations then $\rho = B\rho'B^{-1}$ for some invertible matrix B , and in particular $\ker \rho' = \ker \rho$. Then the equivalence of (iii) and (iv) follows from Theorem 5. On the other hand we have

$$F|_{k_0}\gamma(\tau) = \rho'(\gamma)F(\tau) \quad (\gamma \in \Gamma),$$

so it is clear that the coordinates of F are scalar modular forms on the finite index subgroup $\ker \rho' \subseteq \Gamma$. Therefore (ii) and (iii) are equivalent.

Now suppose that some component f of F is a modular form on a congruence subgroup $\bar{\Gamma}(m)$, say, and assume to begin with that ρ (and therefore also ρ') is *irreducible*. Then the space of functions spanned by $f|_{k_0}\gamma$ ($\gamma \in \Gamma$) coincides with the span of the coordinates of F . Since each $f|_{k_0}\gamma$ is modular on $\bar{\Gamma}(m)$ then the same is true for the coordinates of F . So (i) \Rightarrow (ii) in this case. On the other hand, if ρ is *not* irreducible then $n|3$ by Lemma 4 and (iv) holds. The equivalence of (i)-(iv) follows from what we have established, and the Lemma is thus proved. \square

In the remainder of this section we prove that when n does *not* divide 24, all three coordinates of F have unbounded denominators. As the details are largely the same in the three cases, we explain the argument for the first coordinate in full, and we suppress the details for the other two coordinates.

Remark 19. Chris Marks verified this result earlier in [14] using a different but related method, in all but finitely many cases. The exceptional cases (there are probably many) were not made explicit in [14].

The hypergeometric series that occurs in the first coordinate of F is

$${}_3F_2(a, a + 1/3, a + 2/3; a - b + 1, a - c + 1; K) = 1 + \sum_{m \geq 1} C_m j^{-m},$$

where

$$C_m = \frac{12^{3m}}{m!} \cdot \frac{(a)_m (a + 1/3)_m (a + 2/3)_m}{(a - b + 1)_m (a - c + 1)_m} = \frac{(e - 1)n + 3r}{m!} \cdot \left(\frac{2^8}{n}\right)^m \cdot \prod_{i=2m+e}^{3m+e-2} (ni + 3r).$$

Thus, the first coordinate of F is the following modular form:

$$f_1 := \eta^{2k_0} j^{-\frac{(e-1)n+3r}{3n}} \left(1 + ((e-1)n+3r) \sum_{m \geq 1} \left\{ \frac{2^{8m} \prod_{i=2m+e}^{3m+e-2} (in+3r)}{m!n^m} \right\} j^{-m} \right).$$

Similarly, the second and third coordinates of the vector-valued modular form F are equal to the functions

$$f_2 := \eta^{2k_0} j^{\frac{e-1}{6} + \frac{r}{2n}} \left(1 - ((e-1)n+3r) \sum_{m \geq 1} \left\{ \frac{2^{6m} \prod_{i=m+1}^{3m-1} ((2i+1-e)n-3r)}{(2m)!n^{2m}} \right\} j^{-m} \right),$$

$$f_3 := \eta^{2k_0} j^{\frac{e-4}{6} + \frac{r}{2n}} \left(1 - ((e-4)n+3r) \sum_{m \geq 1} \left\{ \frac{2^{6m} \prod_{i=m}^{3m-1} ((2i+4-e)n-3r)}{(2m+1)!n^{2m}} \right\} j^{-m} \right).$$

Theorem 20. Let $\rho = \text{Ind}_{\Gamma_0(2)}^{\Gamma} \chi$ be as in Theorem 2, write $\chi(\bar{U}) = e^{2\pi ir/n}$ where $0 < r < n$ and $\text{gcd}(r, n) = 1$. Assume that $n \nmid 3$. Let $k_0 = 2, 4$ or 6 denote the minimal weight such that there exist nonzero holomorphic vector-valued modular forms for ρ , write $k_0 = 2e + 4$, and let f_1, f_2 and f_3 be defined as above. Write

$$f_1 = \eta^{2k_0} \cdot \sum_{m \geq 0} \frac{a_m}{n^m m!} q^{m + \frac{r}{n} + \frac{e-1}{3}},$$

$$f_2 = \eta^{2k_0} \cdot \sum_{m \geq 0} \frac{b_m}{n^{2m} (2m)!} q^{m + \frac{r}{n} + \frac{e}{3} - 1},$$

$$f_3 = \eta^{2k_0} \cdot \sum_{m \geq 0} \frac{c_m}{n^{2m} (2m+1)!} q^{m + \frac{r}{n} + \frac{e}{3} - 1}.$$

Let p be a prime dividing n . If $p \neq 2, 3$ then all of a_m, b_m and c_m are congruent to $(24r)^m \pmod{p}$. Otherwise one has:

$$a_m \equiv \begin{cases} (6r)^m & \pmod{3^{m+1}} & p = 3, 3^2 \mid n, \\ 8^m & \pmod{2^{3m+1}} & p = 2, 2^4 \mid n, \end{cases}$$

$$b_m, c_m \equiv \begin{cases} (3r)^{2m} & \pmod{3^{2m+1}} & p = 3, 3^2 \mid n, \\ 2^{6m} & \pmod{2^{6m+1}} & p = 2, 2^4 \mid n. \end{cases}$$

Thus if $n \nmid 24$ then f_1, f_2 and f_3 all have unbounded denominators.

Proof. We give the details of the proof for f_1 . The other cases are analogous. Write $j^{-1} = q(1 + qg(q))$ with $g(q) \in \mathbf{Z}[[q]]$ of the form $-744 + 356652q + O(q^2)$. Then

$$j^{-\frac{3r+(e-1)n}{3n}} = q^{\frac{r}{n} + \frac{e}{3} - 1} \left(1 + \sum_{x \geq 1} \frac{\prod_{i=0}^{x-1} (3r + (2i+e-1)n)}{(3n)^x x!} (qg(q))^x \right)$$

and thus

$$\frac{f_1}{\eta^{2k_0}} = q^{\frac{r}{n} + \frac{e-1}{3}} \left(1 + \sum_{x \geq 1} \frac{\prod_{i=0}^{x-1} (3r + (2i+e-1)n)}{(3n)^x x!} (qg(q))^x \right) \times$$

$$\left(1 + ((e-1)n+3r) \sum_{m \geq 1} \left\{ \frac{2^{8m} \prod_{i=2m+e}^{3m+e-2} (in+3r)}{m!n^m} \right\} (1 + qg(q))^m q^m \right).$$

This gives the following q -expansion for $f_1 \eta^{-2k_0} q^{-\frac{r}{n} - \frac{e-1}{3}}$:

$$1 + \sum_{x \geq 1} \frac{\prod_{i=0}^{x-1} (3r + (2i + e - 1)n)}{(3n)^x x!} (qg(q))^x + ((e-1)n + 3r) \times$$

$$\left(\sum_{m \geq 1} \sum_{y=0}^m \binom{m}{y} \left\{ \frac{2^{8m} \prod_{i=2m+e}^{3m+e-2} (in + 3r)}{m! n^m} \right\} q^{m+y} g(q)^y + \right.$$

$$\left. \sum_{x \geq 1} \sum_{m \geq 1} \sum_{y=0}^m \binom{m}{y} \left\{ \frac{2^{8m} \prod_{i=0}^{x-1} (3r + (2i + e - 1)n) \prod_{i=2m+e}^{3m+e-2} (in + 3r)}{3^x n^{m+x} m! x!} \right\} q^{m+x+y} g(q)^{x+y} \right).$$

Suppose that $p|n$ and $p \neq 2, 3$ or 31 (the prime divisors of 744). Then the coefficient of q^m in this expression is a rational number of the form

$$\frac{(-248)^m \prod_{i=0}^{m-1} (3r + (2i + e - 1)n)}{n^m m!} + ((e-1)n + 3r) \times \left(\frac{2^{8m} \prod_{i=2m+e}^{3m+e-2} (ni + 3r)}{n^m m!} + \right.$$

$$\left. \sum_{s=1}^{m-1} \binom{m}{s} \frac{(-248)^s 2^{8(m-s)} \prod_{i=0}^{s-1} (3r + (2i + e - 1)n) \prod_{i=2(m-s)+e}^{3(m-s)+e-2} (ni + 3r)}{n^m m!} \right)$$

plus terms with lower powers of p in the denominator. This shows that this coefficient is of the form $\frac{a_t}{n^t t!}$ where a_t is an integer congruent mod p to

$$(-744r)^t + (3r)^t \left(2^{8t} + \sum_{s=1}^{t-1} \binom{t}{s} (-248)^s 2^{8(t-s)} \right) \equiv (24r)^t \pmod{p}.$$

This proves the theorem for $p \neq 2, 3, 31$.

If $p = 31$ then the coefficient of q^m in the expression for $f_1 \eta^{-2k_0} q^{-\frac{r}{n} - \frac{e-1}{3}}$ is a rational number of the form $\alpha/n^m m!$, where

$$\alpha = ((e-3)n + 3r) \left(2^{8m} \prod_{i=2m+e}^{3m+e-2} (ni + 3r) \right) \equiv (768r)^m \equiv (24r)^m \pmod{31},$$

plus a rational number with lower powers of 31 in the denominator. This proves the theorem in this case.

Next consider $p = 2$ and suppose that $2^4|n$. Write $n = 2^4 \eta$. Then in this case the q -expansion that we're interested in is

$$1 + \sum_{x \geq 1} \frac{31^x \prod_{i=0}^{x-1} (3r + (2i + e - 1)2^4 \nu)}{(2\nu)^x x!} (qg'(q))^x + ((e-1)2^4 \nu + 3r) \times$$

$$\left(\sum_{m \geq 1} \sum_{y=0}^m \binom{m}{y} \left\{ \frac{(93)^y \prod_{i=2m+e}^{3m+e-2} (2^4 i \nu + 3r)}{m! \nu^m} 2^{4m+3y} \right\} q^{m+y} g'(q)^y + \sum_{x \geq 1} \sum_{m \geq 1} \sum_{y=0}^m \right.$$

$$\left. \binom{m}{y} \frac{(93)^{x+y} 2^{3y+4m-x} \prod_{i=0}^{x-1} (3r + (2i + e - 1)2^4 \nu) \prod_{i=2m+e}^{3m+e-2} (2^4 i \nu + 3r)}{3^x \nu^{m+x} m! x!} q^m (qg'(q))^{x+y} \right).$$

where $g' = g/744$. In this case we see that the coefficient of q^m is of the form

$$\frac{(-31)^m \prod_{i=0}^{m-1} (3r + (2i + e - 1)2^4 \nu)}{(2\nu)^m m!}$$

plus a rational number with fewer powers of 2 in its denominator. Thus, the coefficient is of the form $\alpha/(2\nu)^m m!$ where α is an odd integer, and so if we write it in the form $a_m/n^m m!$ we see that $a_m = 2^{3m}\alpha \equiv 2^{3m} \pmod{2^{3m+1}}$.

Finally consider $p = 3$ and suppose that $3^2|n$. Write $n = 3^2\nu$, so that in this case we're interested in

$$1 + \sum_{x \geq 1} \frac{248^x \prod_{i=0}^{x-1} (r + (2i + e - 1)3\nu)}{(3\nu)^x x!} (qg'(q))^x + ((e - 1)3\nu + r) \times \\ \left(\sum_{m \geq 1} \sum_{y=0}^m \binom{m}{y} \frac{2^{8m} 248^y 3^y \prod_{i=2m+e}^{3m+e-2} (3i\nu + r)}{m!(3\nu)^m} q^{m+y} g'(q)^y + \sum_{x \geq 1} \sum_{m \geq 1} \sum_{y=0}^m \binom{m}{y} \frac{2^{8m} \prod_{i=0}^{x-1} (r + (2i + e - 1)3\nu) \prod_{i=2m+e}^{3m+e-2} (3i\nu + r) 248^{x+y}}{3^{m+x-y} \nu^{m+x} m! x!} q^m (qg'(q))^{x+y} \right).$$

In this case we see that the coefficient of q^m is of the form

$$\frac{(-248)^m \prod_{i=0}^{m-1} (r + (2i + e - 1)3\nu)}{(3\nu)^m m!} + ((e - 1)3\nu + r) \times \left(\frac{2^{8m} \prod_{i=2m+e}^{3m+e-2} (3i\nu + r)}{m!(3\nu)^m} + \sum_{x=1}^{m-1} \binom{m}{x} \frac{2^{8(m-x)} (-248)^x \prod_{i=0}^{x-1} (r + (2i + e - 1)3\nu) \prod_{i=2(m-x)+e}^{3(m-x)+e-2} (3i\nu + r)}{(3\nu)^m m!} \right).$$

plus a rational number with fewer powers of 3 in the denominator. We thus see that the coefficient is of the form $\alpha/(3\nu)^m m!$ where α is an integer satisfying

$$\alpha \equiv r^m \left(1 + 2^{8m} + \sum_{x=1}^{m-1} \binom{m}{x} 2^{8(m-x)} \right) \equiv (2r)^m \pmod{3}$$

Thus, if we write the coefficient as $a_m/n^m m!$ then $a_m \equiv (6r)^m \pmod{3^{m+1}}$. This concludes the proof of the congruences for f_1 , and the final claim follows immediately from them. \square

5. UNBOUNDED DENOMINATORS IN THE GENERAL CASE

In this Section, we consider the question of unbounded denominators for vector-valued modular forms of *arbitrary weight* associated with the induced representation ρ (cf. Proposition 2). Stated in terms of modular forms on $\bar{\Gamma}_0(2)$, the main result is as follows.

Theorem 21. *Let $f \in M_k(\bar{\Gamma}_0(2), \chi)$ be a nonzero holomorphic modular form, where χ is as in (2). Suppose that f has algebraic Fourier coefficients. If p is a prime dividing n , the powers of p that divide the denominators of f are unbounded under any of the following circumstances: $p \geq 5$; $p = 3$ and $p^2|n$; $p = 2$ and $p^4|n$. In particular, the following are equivalent:*

- (a) f has bounded denominators;
- (b) $n|24$;
- (c) f is a congruence modular form.

By Theorem 20, the conclusions of the Theorem hold if, in place of f , we take one of the components f_1, f_2 or f_3 of the vector-valued modular form F that we studied in the previous Section. The idea of the proof of Theorem 21 is to transfer this special result for F into a general result about vector-valued modular forms. The methods for doing this are essentially already in the literature ([16], [15], [5]), though they are not stated in the form that we need here. We will therefore give some of the details.

First we must revert to the original induced representation ρ described in Proposition 2 from the equivalent representation ρ' used in Section 4. We always assume that n does not divide 3, so that ρ is irreducible (Lemma 4). Let

$$\mathcal{H}(\rho) = \bigoplus_{k \geq k_0} \mathcal{H}(k, \rho)$$

be the \mathbf{Z} -graded space of vector-valued modular forms associated with ρ . Similarly, we have $\mathcal{H}(\rho')$. If B is an invertible matrix that intertwines ρ and ρ' , i.e., $B\rho'B^{-1} = \rho$, then the map $F \mapsto BF$ induces an isomorphism of \mathbf{Z} -graded spaces $\mathcal{H}(\rho') \xrightarrow{\cong} \mathcal{H}(\rho)$. We have already pointed out that the minimal weight of a nonzero form in $\mathcal{H}(\rho')$ is $k_0 = 2, 4$ or 6 , so the same is true for $\mathcal{H}(\rho)$. We take the matrix B to be

$$B := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & \epsilon\sigma & -\epsilon\sigma \end{pmatrix},$$

so that $B\rho'(\bar{T})B^{-1} = \rho(\bar{T})$. Because $F := \begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix}$ satisfies $F \in \mathcal{H}(k_0, \rho')$ then $BF \in \mathcal{H}(k_0, \rho)$, and $BF = \begin{pmatrix} f_1 \\ f_2 + f_3 \\ \epsilon\sigma(f_2 - f_3) \end{pmatrix}$. From Theorem 20 we immediately deduce

Lemma 22. *Let $F_0 := BF$ be as above. Then F_0 has algebraic Fourier coefficients. Moreover, if p is a prime dividing n , the powers of p that divide the denominators of the Fourier coefficients of each of the components of F_0 are unbounded under any of the following circumstances: $p \geq 5$; $p = 3$ and $p^2 \mid n$; $p = 2$ and $p^4 \mid n$. \square*

For a field $E \supseteq \mathbf{Q}$ we write

$$(8) \quad \mathcal{H}_E(\rho) := \bigoplus_{k \geq k_0} \mathcal{H}_E(k, \rho),$$

for the \mathbf{Z} -graded space of vector-valued modular forms whose Fourier coefficients lie in E . Let \mathfrak{M}_E be the space of classical modular forms on Γ with Fourier coefficients in E , and let

$$D : \mathcal{H}(k, \rho) \rightarrow \mathcal{H}(k + 2, \rho)$$

be the usual differential operator $D = D_k : f \mapsto q \frac{df}{dq} - \frac{kE_2}{12} f$. The ring of differential operators $\mathfrak{M}_E(D)$ consists of (noncommutative) polynomials in D with coefficients in \mathfrak{M}_E and satisfying $Df - fD = D(f)$. This ring acts naturally on $\mathcal{H}_E(\rho)$, with \mathfrak{M}_E acting componentwise.

We now prove

Theorem 23. *Suppose that $F \in \mathcal{H}(k, \rho)$ has algebraic coefficients. If p is a prime dividing n , the powers of p that divide the denominators of the Fourier coefficients of each of the components of F are unbounded under any of the following circumstances: $p \geq 5$; $p = 3$ and $p^2 \mid n$; $p = 2$ and $p^4 \mid n$.*

Proof. (Cf. Section 3 of [5].) We use the following assertion: (★) if $I \subseteq \mathcal{H}_E(\rho)$ is a nonzero $\mathfrak{M}_E(D)$ -submodule, and if $\Delta = \eta^{24}$ is the usual discriminant, then some power Δ^r of Δ annihilates $\mathcal{H}_E(\rho)/I$. Indeed, the proof given in [5] for the case $E = \mathbb{Q}$ applies in general.

We take $E = \bar{\mathbb{Q}}$ with I the set of forms $G \in \mathcal{H}_{\bar{\mathbb{Q}}}(\rho)$ that do not satisfy the conclusions of the Theorem. So there is an index j and a large enough integer N (depending on G and j) such that the Fourier coefficients of the j^{th} component G_j of G is such that $p^N G_j$ is p -integral. Here, p is a prime divisor of n , as in the statement of Lemma 22.

Now I is an $\mathfrak{M}_{\bar{\mathbb{Q}}}(D)$ -submodule of $\mathcal{H}_{\bar{\mathbb{Q}}}(\rho)$, so by (★) we can conclude that either $I = 0$ or there is an integer r such that $\Delta^r F_0 \in I$, where F_0 is as in Lemma 22. In the latter case, there is a power p^N of p and an index j such that $p^N \Delta^r (F_0)_j$ is p -integral, in which case $p^N (F_0)_j$ is itself p -integral. Because this contradicts Lemma 22, the conclusion is that $I = 0$. The Theorem follows immediately. \square

Finally, suppose that $f \in M_k(\bar{\Gamma}_0(2), \chi)$ is a holomorphic modular form with algebraic Fourier coefficients. By Proposition 2, f is the first component of a vector-valued modular form $F' \in \mathcal{H}_{\bar{\mathbb{Q}}}(k, \rho)$, and we can then apply Theorem 23 to F' to complete the proof of Theorem 21.

6. CONGRUENCES

Let n be a positive integer and let $0 < r < n$ be another integer. Define the character $\chi_{n,r}: \bar{\Gamma}_0(2) \rightarrow \mathbb{C}^\times$ by setting $\chi_{n,r}(\bar{U}) = e^{2\pi i r/n}$ and $\chi_{n,r}(\bar{V}) = -1$. Assume that n is odd and $r > n/2$, so that we are in Case A with a minimal weight of 2 for $\rho = \text{Ind } \chi$. In this case $H_0 = \ker \chi = \langle \bar{U}^n \rangle \Gamma_0(2)'$. Set $X = X_{H_0}$, which is a hyperelliptic curve of genus $g_X = (n-1)/2$ (cf. Theorem 16). One can use Riemann-Roch to show that $S_2(\bar{\Gamma}_0(2), \chi_{n,r})$ is one dimensional for each such pair (n, r) , and we have

$$S_2(H_0) = \bigoplus_{r=(n+1)/2}^{n-1} S_2(\bar{\Gamma}_0(2), \chi_{n,r}).$$

By looking at the first coordinate of the corresponding vector-valued modular forms, one obtains a basis for $S_2(H_0)$ as follows.²

Theorem 24. *Let n be an odd integer that does not divide 3 and set $H_0 = \langle \bar{U}^n \rangle \bar{\Gamma}_0(2)'$. Then $\dim_{\mathbb{C}} S_2(H_0) = (n-1)/2$ and a basis for this space is given by the modular forms*

$$f_{n,r} := \eta^4 K^{\frac{r}{n} - \frac{2}{3}} {}_3F_2 \left(\frac{r}{n} - \frac{2}{3}, \frac{r}{n} - \frac{1}{3}, \frac{r}{n}; \frac{3r}{2n}, \frac{3r}{2n} - \frac{1}{2}; K \right)$$

where r runs from $(n+1)/2$ up to $n-1$.

After Theorem 16 we may also interpret these modular forms as a basis of holomorphic differentials on the smooth projective hyperelliptic curve defined by the affine equation $y^2 = x^n + 64$.

²Let ρ' be a representation equivalent to ρ such that $\rho(\bar{T})$ is diagonal. It was observed above that the first coordinate of a vector-valued modular form for ρ is a modular form on H_0 . This will still be true for the equivalent representation ρ' , and it is this particular representation that is used to prove Theorem 24.

Example 25. The geometric considerations of this paper were inspired by the following computation: let $n = 5$. Then one checks that

$$\dim_{\mathbb{C}} S_k(H_0) = \begin{cases} 2 & k = 2, \\ 6 & k = 4. \end{cases}$$

Since X is hyperelliptic, the canonical embedding is not a closed embedding in this case. To find a projective model for $H_0 \setminus \mathcal{H}^*$, one can instead use modular forms of weight 4.

To describe $S_2(H_0)$ we use the characters $\chi_{(5,3)}$ and $\chi_{(5,4)}$. Let f_1 and f_2 denote the corresponding cusp forms. One finds that

$$\begin{aligned} f_1 &= \eta^4 K^{-\frac{1}{15}} {}_3F_2 \left(-\frac{1}{15}, \frac{4}{15}, \frac{3}{5}; \frac{9}{10}, \frac{2}{5}; K \right) \\ &= q_{10} - \frac{28}{5} q_{10}^{11} + \frac{222}{5^2} q_{10}^{21} + \frac{168}{5^3} q_{10}^{31} - \frac{5071}{5^4} q_{10}^{41} - \frac{123732}{5^6} q_{10}^{51} - \frac{58634}{5^7} q_{10}^{61} + \cdots, \\ f_2 &= \eta^4 K^{\frac{2}{15}} {}_3F_2 \left(\frac{2}{15}, \frac{7}{15}, \frac{4}{5}; \frac{6}{5}, \frac{7}{10}; K \right) \\ &= q_{10}^3 - \frac{4}{5} q_{10}^{13} - \frac{102}{5^2} q_{10}^{23} + \frac{296}{5^3} q_{10}^{33} + \frac{1839}{5^4} q_{10}^{43} + \frac{15324}{5^6} q_{10}^{53} + \frac{463134}{5^7} q_{10}^{63} + \cdots, \end{aligned}$$

where $q_{10} = e^{2\pi iz/10}$. One can similarly show that

$$\begin{aligned} f_3 &= \eta^4 K^{-\frac{1}{6}} {}_2F_1(-1/6, 1/6; 1/2; K), \\ f_4 &= \eta^4 K^{1/3} {}_2F_1(1/3, 2/3; 3/2; K), \end{aligned}$$

describe a basis for $M_2(\bar{\Gamma}(2))$ (see Example 21 of [6]), and the forms f_1, f_2, f_3 and f_4 define a basis for $M_2(H_0)$. The forms

$$\begin{aligned} G_1 &= f_1^2, & G_2 &= f_1 f_2, & G_3 &= f_2^2, \\ G_4 &= f_1 f_3, & G_5 &= f_2 f_3, & G_6 &= f_2 f_4. \end{aligned}$$

then yield a basis for $S_4(H_0)$, and it defines a closed embedding $X \rightarrow \mathbf{P}_{\mathbb{C}}^5$ via

$$z \mapsto (G_1(z) : G_2(z) : G_3(z) : G_4(z) : G_5(z) : G_6(z)).$$

The image is the smooth curve whose zero locus is defined by the homogeneous equations

$$\begin{pmatrix} X_1^2 - X_4 X_5 + 64 X_3 X_6 \\ X_1 X_2 - X_5^2 + 64 X_6^2 \\ -X_2^2 + X_1 X_3 \\ -X_2 X_4 + X_1 X_5 \\ -X_2 X_3 + X_1 X_6 \\ -X_3 X_4 + X_2 X_5 \\ -X_3^2 + X_2 X_6 \\ X_3 X_5 - X_4 X_6 \end{pmatrix}.$$

In the affine chart defined by $X_6 \neq 0$ the curve is given by

$$\{(a^3 : a^2 : a : ab : b : 1) \in \mathbf{P}^5 \mid a^5 - b^2 + 64 = 0\},$$

where $a = X_3/X_6$ and $b = X_5/X_6$. This is as expected by Theorem 16.

Before we state and prove our congruence result we must prepare with some preliminary definitions and results. Let $q = p^r$ be a prime power and let χ denote a character of the cyclic group \mathbf{F}_q^\times . Extend χ to a function on \mathbf{F}_q by setting $\chi(0) = 0$ if $\chi \neq 1$ and $\chi(0) = 1$ otherwise. Recall that the *Gauss sum* $G(\chi)$ of such a character χ is the complex number

$$G(\chi) := \sum_{u \in \mathbf{F}_q} \chi(u) \mathbf{e}(\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(u)/p).$$

If χ' is a second character of \mathbf{F}_q^\times , then the *Jacobi sum* $J(\chi, \chi')$ associated to χ and χ' is the complex number

$$J(\chi, \chi') := \sum_{u_1+u_2=1} \chi(u_1)\chi'(u_2).$$

Lemma 26. *Let χ and χ' be characters of \mathbf{F}_q^\times . If $\chi\chi'$ is nontrivial then*

$$J(\chi, \chi') = \frac{G(\chi)G(\chi')}{G(\chi\chi')}.$$

Proof. Theorem 2.1.3 of [3]. □

Lemma 27. *Let n be an odd positive integer and let p be an odd prime congruent to $-1 \pmod n$. Let $q = p^{2t}$, and let χ be a character of \mathbf{F}_q^\times of order n . Then the Gauss sum $G(\chi)$ satisfies $G(\chi) = (-1)^{t+1}p^t$.*

Proof. See Theorem 11.6.3 of [3]. □

Proposition 28. *Let n be an odd integer and let p be a prime satisfying $p \equiv -1 \pmod n$. Then the numerator of the zeta function of a smooth projective model of the affine curve $y^2 = x^n + 64$ is equal to $L_p(T) = (1 + pT^2)^{(n-1)/2}$.*

Proof. Use results of Weil [18] and the preceding results on Gauss and Jacobi sums. □

An n -term congruence result for weight two modular forms on X follows immediately from Proposition 28 and Theorem 6.1 of [7]. The factorization of the L -function of X into quadratic factors suggests that one might be able to reduce this to a three-term congruence relation of Hecke type. Our next theorem confirms that such congruence relations indeed hold.

Theorem 29. *Let n be an odd integer that does not divide 3, let r denote an integer between $(n+1)/2$ and $n-1$, and let $f_{n,r}$ be a modular form of weight 2 on X as in Theorem 24. Let $N = 2n$ and let $f_{n,r}(q_N) = \sum_{m \geq 1} a_m q_N^m$ denote the q_N -expansion of $f_{n,r}$, where $q_N = e^{2\pi iz/N}$. Then for all primes $p \equiv -1 \pmod n$, and for all indices $m \geq 1$, one has the congruence*

$$a_{p^2 m} + p a_m \equiv 0 \pmod{p^{2+v_p(m)}}.$$

Proof. If $\gcd(n, r) > 1$ then we may replace n and r by $n/\gcd(n, r)$ and $r/\gcd(n, r)$ and work on the curve $y^2 = x^{n/\gcd(n, r)} + 64$. We may thus assume without loss of generality that $\gcd(n, r) = 1$.

Let $G = \bar{\Gamma}_0(2)/H_0 \cong (\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ and let ζ denote a primitive n th root of unity. Then G acts on X via $(r, e) \cdot (x, y) = (\zeta^r x, ey)$. Recall that there is a decomposition

$$S_2(H_0) = \bigoplus_{r=(n+1)/2}^{n-1} S_2(\bar{\Gamma}_0(2), \chi_{n,r})$$

where $S_2(\bar{\Gamma}_0(2), \chi_{n,r})$ is the $\chi_{n,r}$ -isotypic piece of $S_2(H_0)$ under the induced action of the finite abelian group G . Furthermore, each of these pieces is one-dimensional. The idea now is to use this group action and Theorem 6.1 of [7].

Let $p \equiv -1 \pmod{n}$ be a prime, so that if $q = p^2$, then \mathbf{F}_q contains a primitive n th root of unity. Thus, if we now write X_q for the reduction of $X \pmod{p}$, basechanged to \mathbf{F}_q , then G acts on X_q over \mathbf{F}_q . Let F denote the q th power Frobenius. We wish to compute the twisted L -series

$$\begin{aligned} L(X_q, \chi_{n,r}, T) &:= \exp \left(\frac{1}{2n} \sum_{m \geq 1} \frac{T^m}{m} \sum_{g \in G} \text{Tr}(\chi_{n,r}(g^{-1})) |X(\bar{\mathbf{F}}_q)^{F^m g}| \right) \\ &= \exp \left(\frac{1}{2n} \sum_{m \geq 1} \frac{T^m}{m} \sum_{d|n} \sum_{\substack{a=1 \\ \gcd(a, \frac{n}{d})=1}}^{n/d} \frac{\{|X(\bar{\mathbf{F}}_q)^{F^m(ad,0)}| - |X(\bar{\mathbf{F}}_q)^{F^m(ad,1)}|\}}{\zeta^{adr}} \right). \end{aligned}$$

Note that $q \equiv 1 \pmod{n}$ and q odd imply

$$X(\bar{\mathbf{F}}_q)^{F^m(ad,e)} = \{(x, y) \in X(\bar{\mathbf{F}}_q) \mid (\zeta^{ad} F^m(x), (-1)^e F^m(y)) = (x, y)\} \cup \{\infty\}.$$

These conditions force $x \in \mathbf{F}_{q^{mn/d}}$ and $y \in \mathbf{F}_{q^{2m/\gcd(2,e)}}$. Let us now set

$$N(m, ad, e) = |\{(x, y) \in \bar{\mathbf{F}}_q^2 \mid y^2 = x^n + 64 \text{ and } (\zeta^{ad} F^m(x), (-1)^e F^m(y)) = (x, y)\}|$$

so that

$$\begin{aligned} L(X_q, \chi_{n,r}, T) &= \exp \left(\frac{1}{2n} \sum_{m \geq 1} \frac{T^m}{m} \sum_{d|n} \sum_{\substack{a=1 \\ \gcd(a, n/d)=1}}^{n/d} \zeta^{-adr} \{N(m, ad, 0) - N(m, ad, 1)\} \right) \\ &= \exp \left(\frac{1}{n} \sum_{m \geq 1} \frac{T^m}{m} \sum_{d|n} \sum_{\substack{a=1 \\ \gcd(a, n/d)=1}}^{n/d} \zeta^{-adr} \sum_{\substack{u_1 - u_2 = -64 \\ u_1, u_2 \in \mathbf{F}_{q^m}}} N(x^n = u_1; F^m(x) = \zeta^{-ad} x) \kappa(u_2) \right) \end{aligned}$$

where κ denotes the quadratic character of $\mathbf{F}_{q^m}^\times$. If $x^n = u_1$ and $F^m(x) = \zeta^{-ad} x$, then the other solutions of $x^n = u_1$ are the $\zeta^j x$, and $F^m(\zeta^j x) = \zeta^{j-ad} x$. Note that ζ^{-ad} is a primitive (n/d) th root of unity. It follows that the condition $F^m(x) = \zeta^{-ad} x$ forces $\mathbf{F}_{q^{mn/d}} = \mathbf{F}_{q^m}(x)$. These observations show that

$$N(x^n = u_1; F^m(x) = \zeta^{-ad} x) = \frac{1}{\phi(n/d)} N(x^n = u_1; \mathbf{F}_{q^{mn/d}} = \mathbf{F}_{q^m}(x)).$$

In particular, this quantity is independent of a . Note that if m is an integer, and if ζ_m is a primitive m th root of unity, then

$$\sum_{\substack{a=1 \\ \gcd(a,m)=1}}^m \zeta_m^{-ar} = \sum_{a=1}^m \sum_{b|\gcd(a,m)} \mu(b) \zeta_m^{-ar} = \sum_{b|m} \mu(b) \sum_{a=1}^{m/b} \zeta_m^{-abr} = m \sum_{\substack{b|m \\ m|br}} \frac{\mu(b)}{b}$$

where μ is the Moebius function. We thus see that $L(X_q, \chi_{n,r}, T)$ is equal to

$$\exp \left(\frac{1}{n} \sum_{m \geq 1} \frac{T^m}{m} \sum_{d|n} \frac{\mu(d)}{\phi(d)} \sum_{\substack{u_1 - u_2 = -64 \\ u_1, u_2 \in \mathbf{F}_{q^m}}} N(x^n = u_1; \mathbf{F}_{q^{md}} = \mathbf{F}_{q^m}(x)) \kappa(u_2) \right);$$

note that the condition $d|b$ replaced $d|br$, which is permissible since $\gcd(n, r) = 1$.

Define an arithmetic function α as $\alpha(x) = \prod_{p|x} (-1)^{v_p(x)}$. An inclusion-exclusion argument allows one to eliminate the condition $\mathbf{F}_{q^{md}} = \mathbf{F}_{q^m}(x)$. We deduce that

$$\begin{aligned} &L(X_q, \chi_{n,r}, T) \\ &= \exp \left(\frac{1}{n} \sum_{m \geq 1} \frac{T^m}{m} \sum_{d|n} \frac{\mu(d)}{\phi(d)} \sum_{\substack{u_1 - u_2 = -64 \\ u_1, u_2 \in \mathbf{F}_{q^m}}} \sum_{c|d} \alpha(d/c) N(x^n = u_1; x \in \mathbf{F}_{q^{mc}}) \kappa(u_2) \right). \end{aligned}$$

We have $N(x^n = u_1; x \in \mathbf{F}_{q^{mc}}) = \sum_{\chi^{n=1}} \chi(u_1)$, where the sum runs over all characters of $\mathbf{F}_{q^{mc}}^\times$ of order dividing n . Since u_1 is in \mathbf{F}_{q^m} , we'd like to sum over characters of \mathbf{F}_{q^m} instead. The characters of $\mathbf{F}_{q^{mc}}^\times$ of order n restrict to characters of $\mathbf{F}_{q^m}^\times$ of order n/c . Applications of Lemmas 26 and 27 yield

$$\sum_{\chi^{n/c=1}} \sum_{\substack{u_1 - u_2 = -64 \\ u_1, u_2 \in \mathbf{F}_{q^m}}} \chi(u_1) \kappa(u_2) = \sum_{\chi^{n/c=1}} (-1)^{m+1} p^m,$$

so that we deduce

$$L(X_q, \chi_{n,r}, T) = \exp \left(- \sum_{m \geq 1} \frac{(-pT)^m}{m} \sum_{d|n} \frac{\mu(d)}{\phi(d)} \sum_{c|d} \alpha(d/c) \right).$$

Note that

$$\sum_{c|d} \alpha(c) = \prod_{p|d} \sum_{t=0}^{v_p(d)} \alpha(p^t) = \prod_{p|d} \frac{(-1)^{v_p(d)} + 1}{2} = \begin{cases} 1 & d = z^2, \\ 0 & d \neq z^2. \end{cases}$$

Since the Moebius function μ vanishes on squares, save for $\mu(1) = 1$, we conclude that $L(X_q, \chi_{n,r}, T) = 1 + pT$. Theorem 6.1 of [7] now implies that $a_{mp^2} + pa_m \equiv 0 \pmod{p^{2+v_p(m)}}$ for all $m \geq 1$. \square

Remark 30. It would be of interest to find a proof of Theorem 29 that uses our explicit formulae for the modular forms $f_{n,r}$ in place of the use of Theorem 6.1 of [7]. Presumably such a proof would then generalize to Cases B and C of this paper, where the minimal weights are 4 and 6. For this it might be useful to note that $\eta(6\tau)^4$ is the newform corresponding to the elliptic curve $y^2 = x^3 + 1$ of conductor 36, whose q -expansion is well-understood (cf. Proposition 8.5.3 of [4]).

REFERENCES

- [1] A. O. L. Atkin, Wen-Ching Winnie Li, and Ling Long. On Atkin and Swinnerton-Dyer congruence relations. II. *Math. Ann.*, 340(2):335–358, 2008.
- [2] A. O. L. Atkin and H. P. F. Swinnerton-Dyer. Modular forms on noncongruence subgroups. In *Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968)*, pages 1–25. Amer. Math. Soc., Providence, R.I., 1971.

- [3] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication.
- [4] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.
- [5] Cameron Franc and Geoffrey Mason. Fourier coefficients of vector-valued modular forms of dimension 2. *Canad. Math. Bull.*, 57(3):485–494, 2014.
- [6] Cameron Franc and Geoffrey Mason. Hypergeometric series, modular linear differential equations, and vector-valued modular forms. *Ramanujan Journal*, (to appear).
- [7] Nicholas M. Katz. Crystalline cohomology, Dieudonné modules, and Jacobi sums. In *Automorphic forms, representation theory and arithmetic (Bombay, 1979)*, volume 10 of *Tata Inst. Fund. Res. Studies in Math.*, pages 165–246. Tata Inst. Fundamental Res., Bombay, 1981.
- [8] Chris Kurth and Ling Long. On modular forms for some noncongruence subgroups of $SL_2(\mathbb{Z})$. II. *Bull. Lond. Math. Soc.*, 41(4):589–598, 2009.
- [9] Chris A. Kurth and Ling Long. On modular forms for some noncongruence subgroups of $SL_2(\mathbb{Z})$. *J. Number Theory*, 128(7):1989–2009, 2008.
- [10] Wen-Ching Winnie Li and Ling Long. Fourier coefficients of noncongruence cuspforms. *Bull. Lond. Math. Soc.*, 44(3):591–598, 2012.
- [11] Wen-Ching Winnie Li, Ling Long, and Zifeng Yang. On Atkin-Swinnerton-Dyer congruence relations. *J. Number Theory*, 113(1):117–148, 2005.
- [12] Ling Long. On Atkin and Swinnerton-Dyer congruence relations. III. *J. Number Theory*, 128(8):2413–2429, 2008.
- [13] Christopher Marks. Irreducible vector-valued modular forms of dimension less than six. *Illinois J. Math.*, 55(4):1267–1297 (2013), 2011.
- [14] Christopher Marks. Fourier coefficients of three-dimensional vector-valued modular forms. *Preprint*, 2012.
- [15] Christopher Marks and Geoffrey Mason. Structure of the module of vector-valued modular forms. *J. Lond. Math. Soc. (2)*, 82(1):32–48, 2010.
- [16] Geoffrey Mason. On the Fourier coefficients of 2-dimensional vector-valued modular forms. *Proc. Amer. Math. Soc.*, 140(6):1921–1930, 2012.
- [17] A. J. Scholl. Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences. *Invent. Math.*, 79(1):49–77, 1985.
- [18] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.