Journal of Algebra **214,** 276–300 (1999)
Article ID jabr.1998.7678, available online at http://www.idealibrary.com on IDEAL®

Fake Congruence Modular Curves and Subgroups of the Modular Group*

Gabriel Berger†

*Department of Mathematics, University of California at Irvine,
Irvine, California 92697-3875*
E-mail: gberger@math.uci.edu

Communicated by Walter Feit

Received April 13, 1998

We construct a special class of noncongruence modular subgroups and curves, analogous in some ways to the usual congruence ones. The subgroups are obtained via the Burau representation, and the associated quotient curves have a natural moduli space interpretation. In fact, they are reduced Hurwitz spaces corresponding to covers with 4 branch points and monodromy group equal to semi-direct products of a cyclic and an abelian group. Furthermore, they form a modular tower in the sense of Fried. We study representations on the cohomology of these fake congruence modular curves and also calculate the genera of certain quotient curves. © 1999 Academic Press

Key Words: Burau representation; fake congruence subgroup; Hurwitz space; modular tower.

1. INTRODUCTION

The present work has two starting points. The first is the work of Oda and Terasoma on the Burau representation of the Artin braid group B_n. This representation is, in general, a homomorphism

$$\pi_n \colon B_n \to GL_{n-1}(\mathbb{Z}[t, t^{-1}]). \tag{1}$$

* Supported in part by JSPS Grant P94015 and NSA Grant 032596.

† The author expresses his thanks and acknowledges his debts to Takayuki Oda for introducing the topics considered in this paper and to Mike Fried for valuable discussions regarding Hurwitz spaces and connections with the modular group. We note that similar topics have been considered earlier by Helmut Voelklein, whose primary interest was the realization of certain finite groups of Lie type as Galois groups over $\mathbb{Q}$.

0021-8693/99 $30.00

However, in [O-T] and this paper, it is shown that under certain conditions and for certain prime powers q, the map π_3 induces a surjective homomorphism

$$\pi\colon PSL_2(\mathbb{Z}) \to PSL_2(\mathbb{F}_q), \tag{2}$$

where $\mathbb{F}_q$ is the finite field with q elements in it. (In fact, we can define such a π in more generality. But then all we would know about its image is that it is a certain unitary subgroup of $PGL_2(\mathbb{Z}[\zeta]/\mathscr{N})$, where ζ is a root of unity and $\mathscr{N}$ is an ideal in $\mathbb{Z}[\zeta]$.) Recall that $PSL_2(\mathbb{Z})$ is generated by the images mod $\langle \pm 1\rangle$ of

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad U = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$

with the relations $(SU)^3 = (SUS)^2 = 1$. (Here and subsequently, all matrices will be taken mod $\langle \pm 1\rangle$.) Thus B_3 maps surjectively onto $PSL_2(\mathbb{Z})$ via

$$\sigma_1 \mapsto S, \qquad \sigma_2 \mapsto U. \tag{3}$$

The kernel is the center $Z(B_3)$, which is generated by $(\sigma_1\sigma_2)^3$.

The second starting point is the following result of Fried [F], which gives a new, combinatorial group-theoretic way to approach congruence subgroups. Suppose N is an odd integer and D_N is the dihedral group

$$\langle \gamma, t\colon \gamma^2 = t^N = 1,\ \gamma t \gamma^{-1} = t^{-1}\rangle. \tag{4}$$

Observe that D_N is the semi-direct product of $\mathbb{Z}/N$ and $\mathbb{Z}/2$. Embed D_N in the symmetric group S_N via the permutation representation on the N cosets of $\langle\gamma\rangle$, and take $\mathscr{C}$ to be the conjugacy class of involutions. Let X be the set

$$\{(a,b,c,d) \in \mathscr{C}^4\colon \langle a,b,c,d\rangle = D_N, \quad \text{and} \quad a\cdot b\cdot c\cdot d = 1\}/N_{S_N}(\mathscr{C}), \tag{5}$$

where $N_{S_N}(\mathscr{C})$ is the normalizer of $\mathscr{C}$ in S_N. We can define a right action of $PSL_2(\mathbb{Z})$ on X via

$$(a,b,c,d)S = (aba^{-1}, a, c, d) \tag{6}$$

$$(a,b,c,d)U = (a, bcb^{-1}, b, d). \tag{7}$$

Fried's theorem then states that the stabilizer of the element

$$(\gamma, \gamma, t\gamma, t\gamma) \qquad \text{mod } N_{S_N}(\mathscr{C}) \tag{8}$$

is $\Gamma_0(N)$.

In fact, in [F, B-F] it is shown that given any transitive subgroup G of S_n and conjugacy classes $(\mathscr{C}_1, \dots, \mathscr{C}_4)$ of G, we can obtain a finite-index subgroup Δ of $SL_2(\mathbb{Z})$. Moreover, the associated quotient curve $\mathfrak{h}/\Delta$ has a moduli space interpretation. We therefore obtain a way of generating noncongruence subgroups of $SL_2(\mathbb{Z})$ with additional structure associated to them.

In [B2], the following is shown. Suppose G is the semi-direct product $\mathbb{Z}[\zeta]/\mathscr{N} \rtimes (\mathbb{Z}[\zeta]/\mathscr{N})^*$, for d an integer and $\mathscr{N}$ an ideal of $\mathbb{Z}[\zeta]$ relatively prime to d. Let $(\mathscr{C}_1, \dots, \mathscr{C}_4) = (\mathscr{C}, \mathscr{C}, \mathscr{C}, \mathscr{C}^{-3})$, with $\mathscr{C}$ the conjugacy class of ζ. Then our Δ is in fact equal to the stabilizer of $\infty \in \mathbb{P}^1(\mathbb{Z}[\zeta]/\mathscr{N})$. That is, $\Delta = \pi^{-1}(B)$, where B is the standard Borel subgroup

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

of $PGL_2(\mathbb{Z}[\zeta]/\mathscr{N})$ and π is the map obtained from the Burau representation as above. Equivalently, $\mathfrak{h}/\Delta$ is a course moduli space for Kummer covers X of $\mathbb{P}^1$ together with a subgroup of $J(X)$ isomorphic to $\mathbb{Z}[\zeta]/\mathscr{N}$. If $G = D_N$, then Δ is just $\Gamma_0(N)$. We thus obtain a noncongruence modular curve with a moduli space interpretation which generalizes $X_0(N)$. Furthermore, if we fix d and let N vary through powers of a prime p, then for certain p we obtain a modular tower (see [F2]).

It is our hope that these so-called "fake congruence subgroups and modular curves" will provide a fertile testing ground for many of the objects and theories associated with the usual congruence ones (Hecke operators, action of Frobenius, ...). Accordingly, we have begun their study in this paper.

The contents are as follows: in Section 2, we outline the basic framework in which we intend this work to be considered, including a review of Hurwitz spaces and their relation to noncongruence modular curves. In Section 3, we use the Oda–Terasoma theorem to construct fake congruence subgroups and fake congruence modular curves. In Section 4, we determine the character multiplicities of the representation of $PSL_2(\mathbb{F}_q)$ on the cohomology of our fake congruence modular curves. Finally, in Section 5, we determine the genera of various quotient curves.

2. HURWITZ SPACES OF FOUR-BRANCH POINT COVERS AND FAKE CONGRUENCE SUBGROUPS

2.1. *Review of Hurwitz Spaces.* The references for this section are [B-F, F-V]. Let G be a finite group embedded as a transitive subgroup of S_n for some positive integer n. Let $\mathbf{C} = (\mathscr{C}_1, \dots, \mathscr{C}_4)$ e a quadruple of conjugacy classes of G. We are interested in parametrizing covers of $\mathbb{P}^1$ (over $\mathbb{C}$)

ramified over four points with monodromy group G and ramification data $\mathbf{C}$. To do so, we introduce the following definitions.

DEFINITION 1. We set $U^4 = \{(z_1, \ldots, z_4) \in (\mathbb{P}^1)^4\colon\ z_i \neq z_j \text{ for } i \neq j\}$, and let $U_4 = U^4/S_4$ denote the natural quotient. The *Nielsen class* associated to the data $(G, \mathbf{C})$ is $Ni(G, \mathbf{C})$ and is

$$\big\{(g_1, \ldots, g_4) \in G^4\colon \langle g_1, \ldots, g_4\rangle = G,\ g_1 \cdots g_4 = 1 \\ \text{and} \quad g_i \in \mathscr{C}_{i\sigma} \quad \text{for some } \sigma \in S_4\big\}.$$

We also set $Ni(G, \mathbf{C})^{ab} = Ni(G, \mathbf{C})/N_{S_n}(\mathbf{C})$, where $N_{S_n}(\mathbf{C})$ is the normalizer of $\mathbf{C}$ in S_n. Finally, the Hurwitz monodromy group H_4 is the fundamental group of U_4. It has the presentation

$$\langle Q_1, Q_2, Q_3\colon Q_iQ_{i+1}Q_i = Q_{i+1}Q_iQ_{i+1},\ Q_1Q_3 \\ = Q_3Q_1,\ Q_1Q_2Q_3Q_3Q_2Q_1 = 1\rangle.$$

Note that H_4 is very closely related to B_3, since B_3 is the fundamental group of unordered, distinct triples of $\mathbb{C}^1 = \mathbb{P}^1 - \{\infty\}$. In fact, Hurwitz space theory can be formulated using B_3 instead of H_4.

We have an action of H_4 on $Ni(G, \mathbf{C})^{ab}$ as follows: if $(g_1, \ldots, g_4) \in Ni(G, \mathbf{C})^{ab}$, then

$$(g_1, \ldots, g_4)Q_i = \big(g_1, \ldots, g_{i-1}, g_ig_{i+1}g_i^{-1}, g_i, g_{i+2}, \ldots, g_4\big).$$

(Thus Q_i sends g_i to $g_ig_{i+1}g_i^{-1}$, sends g_{i+1} to g_i, and fixes the other two elements of the quadruple.) Since H_4 is the fundamental group of U_4, each of its orbits on $Ni(G, \mathbf{C})^{ab}$ corresponds to a connected cover of U_4. Let $\mathscr{H}(G, \mathbf{C})$ denote the disjoint union of these covers.

THEOREM 1 [F-V]. *$\mathscr{H}(G, \mathbf{C})$ is a coarse moduli space for covers of $\mathbb{P}^1$ with monodromy group G and ramification data $\mathbf{C}$.*

In fact, this theorem holds for covers with an arbitrary number of branch points.

2.2. $\mathrm{PSL}_2(\mathbb{C})$ *Action.* We have canonical $PSL_2(\mathbb{C})$ actions on U^4, U_4, and $\mathscr{H} = \mathscr{H}(G, \mathbf{C})$ as above: if $\gamma \in PSL_2(\mathbb{C})$, then $\gamma(a, b, c, d) = (\gamma a, \gamma b, \gamma c, \gamma d)$. Also, given a cover $\phi\colon X \to \mathbb{P}^1$, γ acts on this cover by taking it to the composite $\gamma\phi$. We denote the quotients of these actions by $U^{4\,red}$, U_4^{red}, and $\mathscr{H}^{red}$, respectively. The following result is due to Thompson (see [F]).

PROPOSITION 1. *There is a surjective homomorphism*

$$\phi\colon H_4 \to PSL_2(\mathbb{Z})$$

given by

$$\phi(Q_1) = S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \phi(Q_2) = U = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$
$$\phi(Q_3) = S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The kernel is the quaternion group Q_8 *of order* 8.

THEOREM 2 [B-F]. *Suppose* $\mathscr{H}_O$ *is a connected component of* $\mathscr{H}$. *Then there exists a subgroup* Δ *of finite index in* $PSL_2(\mathbb{Z})$ *such that we have the following commutative diagram*:

$$\begin{tikzcd} \mathscr{H}_O^{red} \arrow[r] \arrow[d] & \mathfrak{h}/\Delta \arrow[d] \\ U_4^{red} \arrow[r] & \mathfrak{h}/PSL_2(\mathbb{Z}) \end{tikzcd}$$

The horizontal maps are isomorphisms, and the bottom isomorphism is obtained by taking any $\{a, b, c, d\}$ *to the unique* (*up to isomorphism*) *elliptic curve ramified over* $\{a, b, c, d\}$. *Furthermore,* Δ *arises as follows*: *by construction,* $\mathscr{H}_0^{red}$ *corresponds to a subgroup of finite index* Σ *in* H_4. *Then* $\Delta = \phi(\Sigma)$, *where* ϕ *is the homomorphism of Proposition* 1.

2.3. *The Semidirect Product of Two Abelian Groups and the Burau Representation.* Our general set up is as follows. Suppose $d \geq 1$ is an integer, and ζ is a primitive dth root of unity. Let $\mathscr{N}$ be an ideal of $\mathbb{Z}[\zeta]$ coprime to d, and by abuse of notation, continue to denote the image of ζ in $\mathbb{Z}[\zeta]/\mathscr{N}$ by ζ. Subsequently, by $\mathbb{Z}[\zeta]/\mathscr{N}$ we will mean the additive group of $\mathbb{Z}[\zeta]/\mathscr{N}$ unless otherwise noted; $(\mathbb{Z}[\zeta]/\mathscr{N})^*$ will denote the multiplicative group of (the ring) $\mathbb{Z}[\zeta]/\mathscr{N}$. We can embed $(\mathbb{Z}[\zeta]/\mathscr{N})^*$ into the automorphism group of $\mathbb{Z}[\zeta]/\mathscr{N}$ by setting $\gamma(x) = \gamma x$ for $\gamma \in (\mathbb{Z}[\zeta]/\mathscr{N})^*$ and $x \in \mathbb{Z}[\zeta]/\mathscr{N}$. Thus we may form the semidirect product

$$\mathbb{Z}[\zeta]/\mathscr{N} \rtimes (\mathbb{Z}[\zeta]/\mathscr{N})^*.$$

This group is generated by $\mathbb{Z}[\zeta]/\mathscr{N}$ and symbols $[\gamma]$ for $\gamma \in (\mathbb{Z}[\zeta]/\mathscr{N})^*$, with the relations

$$[\gamma][\alpha] = [\gamma\alpha] \quad \text{for } \alpha \in (\mathbb{Z}[\zeta]/\mathscr{N})^*$$
$$\text{and} \qquad [\gamma]^{-1}t[\gamma] = \gamma t \quad \text{for} \quad t \in \mathbb{Z}[\zeta]/\mathscr{N}.$$

(In the second equality, the left-hand multiplication is in $\mathbb{Z}[\zeta]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta]/\mathcal{N})^*$, and the right-hand multiplication is in the ring $\mathbb{Z}[\zeta]/\mathcal{N}$.) Let G be the subgroup $\mathbb{Z}[\zeta]/\mathcal{N} \rtimes \langle \zeta \rangle$ of $\mathbb{Z}[\zeta]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta]/\mathcal{N})^*$. Notice that $\mathbb{Z}[\zeta]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta]/\mathcal{N})^*$ acts on $\mathbb{Z}[\zeta]/\mathcal{N}$ as a set: the additive group $\mathbb{Z}[\zeta]/\mathcal{N}$ acts upon itself by addition, and the multiplicative group $(\mathbb{Z}[\zeta]/\mathcal{N})^*$ acts on $\mathbb{Z}[\zeta]/\mathcal{N}$ by multiplication. Thus if $\#\mathbb{Z}[\zeta]/\mathcal{N} = N$, we obtain an embedding of $\mathbb{Z}[\zeta]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta]/\mathcal{N})^*$ and its subgroup G into S_N, given as follows: if $t \in \mathbb{Z}[\zeta]/\mathcal{N}$ and $x[\gamma] \in \mathbb{Z}[\zeta]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta]/\mathcal{N})^*$, then

$$t(x[\gamma]) = (t+x)[\gamma].$$

Identify $\mathbb{Z}[\zeta]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta]/\mathcal{N})^*$ and G with their images in S_N. Let $\mathcal{C}$ be the conjugacy class of $[\zeta]$. Set $\mathbf{C} = (\mathcal{C}_1, \dots, \mathcal{C}_4) = (\mathcal{C}, \mathcal{C}, \mathcal{C}, \mathcal{C}^{-3})$.

Now let

$$X = Ni(G, \mathbf{C})^{ab}/Q_8, \tag{9}$$

where Q_8 is the kernel of ϕ as in Proposition 1. Then we have a well-defined action of $PSL_2(\mathbb{Z})$ on X.

THEOREM 3 [B2]. (1) *The action of $PSL_2(\mathbb{Z})$ on X is transitive.*

(2) *We can identify X with $\mathbb{P}^1(\mathbb{Z}[\zeta]/\mathcal{N})$. Furthermore, we have the following commutative diagram, where the right hand map π is as defined in Subsection* 3.2 *and the left hand map is as described in the Introduction.*

$$\begin{tikzcd}
PSL_2(\mathbb{Z}) \arrow[r, "id"] \arrow[d] & PSL_2(\mathbb{Z}) \arrow[d, "\pi"] \\
\mathrm{Aut}(X) \arrow[r] & PGL_2(\mathbb{Z}[\zeta_d]/\mathcal{N})
\end{tikzcd}$$

In addition, the stabilizer of the image of $(\gamma, \gamma^{-1}, t\gamma, \gamma^{-1}t^{-1})$ in X is equal to the subgroup

$$\Gamma_0(\mathcal{N}) = \{\alpha \in PSL_2(\mathbb{Z}) \colon \pi(\alpha)\infty = \infty\}.$$

(3) *The curve $Y_0(\mathcal{N}) = \mathfrak{h}/\Gamma_0(\mathcal{N})$ is a reduced Hurwitz space for covers of $\mathbb{P}^1$ with monodromy group G and ramification data $\mathbf{C}$. Thus each point on $Y_0(\mathcal{N})$ corresponds to an equivalence class of diagrams of the following form*:

$$\begin{tikzcd}
Y \arrow[r, "\alpha"] \arrow[d] & X \arrow[d, "\gamma"] \\
W \arrow[r, "\beta"] & \mathbb{P}^1
\end{tikzcd}$$

We require all maps to be ramified over 4 *points, and the vertical maps to be Galois, with monodromy group* $\mathbb{Z}/d\mathbb{Z} = \langle \zeta \rangle$. *In addition, the map* γ *should have ramification data of the form* $(\zeta, \zeta, \zeta, \zeta^{-3})$ (*here,* ζ *is its own conjugacy class in* $\mathbb{Z}/d\mathbb{Z} = \langle \zeta \rangle$). *Furthermore,* α *must be Galois with group* $\mathbb{Z}[\zeta]/\mathscr{N}$. *Finally, we require* β *to have monodromy group* G *and ramification data* $(\mathscr{C}, \mathscr{C}, \mathscr{C}, \mathscr{C}^{-3})$.

We note that once we specify the map β, Y *and* X *will be uniquely determined. Two diagrams are considered to be equivalent if and only if the lower horizontal maps are equivalent* mod $PSL_2(\mathbb{C})$.

3. CONSTRUCTION OF THE $\Gamma(\mathscr{N})$

3.1. *Fake Congruence Subgroups.* To begin with, we fix natural numbers $n \geq 3$, $d \geq 7$, a primitive dth root of unity ζ, $K = \mathbb{Q}(\zeta)$, $F = \mathbb{Q}(\zeta + \zeta^{-1})$, $\mathscr{N}^+ \subset \mathscr{O}_F$ an ideal, and $\mathscr{N} = \mathscr{N}^+ \mathscr{O}_K$.

Let B_n denote the Artin braid group

$$\langle \sigma_1, \dots \sigma_{n-1} \colon \sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{for} \quad |i-j| > 1 \qquad \text{and} \quad \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \rangle.$$

The reduced Burau representation (see [Bi]) is a homomorphism π_n: $B_n \to GL_{n-1}(\mathbb{Z}[t, t^{-1}])$. It can be obtained, among other methods, via the Fox free calculus, or from the action of B_n on the homology of an infinite cyclic extension of $\mathbb{P}^1$ ramified over $n+1$ points. Its action on the generators of B_n is given as

$$\sigma_1 \mapsto \begin{bmatrix} -t & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\sigma_r \mapsto \begin{bmatrix} 1_{r-2} & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \cdots & t & -t & 1 & 0 \\ \cdots & 0 & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1_{n-r-2} \end{bmatrix} \qquad (1 < r < n-1)$$

and

$$\sigma_{n-1} \mapsto \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & t & -t \end{bmatrix}.$$

Setting $t = \zeta$ and reducing by $\mathscr{N}$ gives us a map $\mathbb{Z}[t, t^{-1}] \to \mathscr{O}_K/\mathscr{N}$, and hence a map $GL_n(\mathbb{Z}[t, t^{-1}]) \to GL_n(\mathscr{O}_K/\mathscr{N})$. We then obtain a new map

$$\pi_{n,\mathscr{N}}\colon B_n \to GL_{n-1}(\mathscr{O}_K/\mathscr{N})$$

by composing with the Burau representation.

Now suppose $n = 3$. In this case we can describe our map as follows. First, notice that B_3 has presentation $\langle \sigma_1, \sigma_2\colon \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \rangle$. Then $\pi_{3,\mathscr{N}}$ is given by

$$\sigma_1 \to \begin{pmatrix} -\zeta & 1 \\ 0 & 1 \end{pmatrix} \tag{10}$$

$$\sigma_2 \to \begin{pmatrix} 1 & 0 \\ \zeta & -\zeta \end{pmatrix}. \tag{11}$$

where we understand the matrix entries to be elements of $\mathscr{O}_K/\mathscr{N}$.

Recall that $Z(B_3)$ is generated by $(\sigma_1\sigma_2)^3$ and observe that

$$\pi_{3,\mathscr{N}}\left((\sigma_1\sigma_2)^3\right) = \begin{pmatrix} \zeta^3 & 0 \\ 0 & \zeta^3 \end{pmatrix}.$$

Thus $\pi_{3,\mathscr{N}}$ induces a map

$$\pi_{\mathscr{N}}\colon PSL_2(\mathbb{Z}) = B_3/Z(B_3) \to PGL_2(\mathscr{O}_K/\mathscr{N}). \tag{12}$$

DEFINITION 2. We have the following analogs of congruence groups and modular curves:

(1) $\Gamma(\mathscr{N}) = \ker(\pi_{\mathscr{N}})$

(2) $\Gamma_0(\mathscr{N}) = \{\gamma \in PSL_2(\mathbb{Z})\colon \ \pi_{\mathscr{N}}(\gamma)\infty = \infty$ (where we take $\infty \in \mathbb{P}^1(\mathscr{O}_K/\mathscr{N})$)

(3) $X(\mathscr{N}) = \mathfrak{h}^*/\Gamma(\mathscr{N})$

(4) $X_0(\mathscr{N}) = \mathfrak{h}^*/\Gamma_0(\mathscr{N})$

(5) $Y(\mathscr{N}) = \mathfrak{h}/\Gamma(\mathscr{N})$

(6) $Y_0(\mathscr{N}) = \mathfrak{h}/\Gamma_0(\mathscr{N})$.

Any subgroup of $PSL_2(\mathbb{Z})$ that contains $\Gamma(\mathscr{N})$ for some $\mathscr{N}$ will be called a *fake congruence subgroup*.

If $d = 2$, we obtain the usual congruence objects with $\mathscr{N}$ replaced by N.

Recall that $PSL_2(\mathbb{Z})$ is the free product of the group of order 2 generated by $USU = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and the group of order 3 generated by $SU = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)$.

Definition 3. Let k be a positive integer. The *Hecke Triangle Group* $T(2,3,k)$ is the group

$$\langle \beta_2, \beta_3, \beta_k \colon \beta_2^2 = \beta_3^3 = \beta_k^k = \beta_2 \beta_3 \beta_k = 1 \rangle.$$

We have a canonical surjection $\psi \colon PSL_2(\mathbb{Z}) \to T(2,3,k)$ given by

$$USU = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \mapsto \gamma_2, \qquad SU = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \mapsto \gamma_3.$$

Since $S = (USUSU)^{-1}$ and $\gamma_k = \gamma_3^{-1}\gamma_2^{-1}$, we also see that $\psi(S) = \gamma_k$.

Now note that in our map $\pi_{\mathscr{N}} \colon PSL_2(\mathbb{Z}) \to PGL_2(\mathbb{Z}[\zeta]/\mathscr{N})$, we have

$$\pi_{\mathscr{N}}(S^r) = \pi_{3,\mathscr{N}}(\sigma_1^r) = \begin{pmatrix} (-\zeta)^r & ((-\zeta)^r - 1)/(-\zeta - 1) \\ 0 & 1 \end{pmatrix}. \tag{13}$$

Thus if we set $k = \#\langle -\zeta \rangle$, then $\pi_{\mathscr{N}}(S^k) = 1$, and so $\pi_{\mathscr{N}}$ factors through $T(2,3,k)$. We set

$$\Delta(\mathscr{N}) = \ker\bigl(T(2,3,k) \to PGL_2(\mathbb{Z}[\zeta]/\mathscr{N})\bigr). \tag{14}$$

3.2. *The Oda–Terasoma Theorem.* By the results of [O-T], the image of B_n under π_n is unitary with respect to a certain hermitian form $H \in GL_{n-1}(\mathbb{Z}[t, t^{-1}])$. (Here, conjugation is the map $t \mapsto t^{-1}$.) H is given by

$$\begin{bmatrix} 1 & -\dfrac{1}{t+1} & 0 & 0 & \cdots \\ -\dfrac{1}{t^{-1}+1} & 1 & -\dfrac{1}{t+1} & 0 & \cdots \\ 0 & -\dfrac{1}{t^{-1}+1} & 1 & -\dfrac{1}{t+1} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{bmatrix}. \tag{15}$$

This form then descends to a form in $GL_{n-1}(\mathscr{O}_K/\mathscr{N})$ (also denoted H). In fact, one can show that the image of $\pi_{n,\mathscr{N}}$ is contained in

$$U_{n-1}(\zeta, H, \mathscr{O}_K/\mathscr{N}) = \bigl\{ g \in GL_{n-1}(\mathscr{O}_K/\mathscr{N}) \colon \bar{g}^t H g = H, \det g \in \langle -\zeta \rangle \bigr\}.$$

The main theorem of [O-T] is that under certain conditions, B_n actually surjects onto $U_{n-1}(\zeta, H, \mathscr{O}_K/\mathscr{N})$.

Theorem 4 [O-T]. *Assume $n \geq 3$, $d \geq 7$ if d is odd, $d \geq 14$ if d is even, $\mathscr{N}$ is coprime with d and $((1 - \zeta^i)/(1 - \zeta))$ $(2 \leq i \leq n)$, the prime factors $\mathfrak{q}$ of $\mathscr{N}$ dividing 6 satisfy $N_{K/\mathbb{Q}}(\mathfrak{q}) \geq 10$, $\mathscr{N}$ is coprime to $n - 4$, and d is odd when $n = 4$. Then*

$$\pi_{n,\mathscr{N}} \colon B_n \to U_{n-1}(\zeta, H, \mathscr{O}_K/\mathscr{N})$$

is surjective.

A special case of this is the following.

THEOREM 5. *Hypotheses as above, suppose $n = 3$ and $\mathcal{N}^+$ is a prime ideal $\mathfrak{p}^+$. Set $\mathfrak{p} = \mathfrak{p}^+\mathcal{O}_K$. Then the map*

$$\pi_{\mathfrak{p}}\colon PSL_2(\mathbb{Z}) \to PU_2(\zeta, H, \mathcal{O}_K/\mathfrak{p})$$

is surjective.

3.3. *Analysis of π_3.* We must now analyze π_3 in more detail.

LEMMA 1. *Let $f = \operatorname{ord}_d p = \min\{a \in \mathbb{N}\colon\ p^a \equiv 1 \bmod d\}$. Let $\mathfrak{p}^+ \subset \mathcal{O}_F$ be a prime over p. Then $\mathfrak{p}^+$*

(1) *remains prime in $\mathcal{O}_K$ if f is even, and $\#(\mathcal{O}_K/\mathfrak{p}^+\mathcal{O}_K) = p^f$, $\#\mathcal{O}_F/\mathfrak{p}^+ = p^{f/2}$,*

(2) *splits into two primes in $\mathcal{O}_K$ if f is odd, and $\#(\mathcal{O}_F/\mathfrak{p}^+) = p^f$.*

Proof. Let

$$T^+(X) = \prod_{\substack{(i,d)=1\\ 0<i<d/2}} \left(X - (\zeta^i + \zeta^{-i})\right)$$

be the irreducible polynomial of $\zeta + \zeta^{-1}$ over $\mathbb{Z}$. We must factor T^+ in $\mathbb{F}_p[X]$; the degree of each factor will be the residue field index of $\mathfrak{p}^+$ (see [C]).

Choose a primitive dth root of unity $\gamma \in \overline{\mathbb{F}}_p$. Then

$$T^+(X) = \prod_{\substack{(i,d)=1\\ 0<i<d/2}} \left(X - (\gamma^i + \gamma^{-i})\right)$$

is a factorization of T^+ over $\overline{\mathbb{F}}_p$. Consider

$$\prod_{0\le j<f} \left(X - \left(\gamma^{p^j} + \gamma^{-p^j}\right)\right) \in \mathbb{F}_p[X].$$

This is irreducible if and only if f is odd (otherwise, it will be a square). Thus $f(\mathfrak{p}^+/p) = f/2$ if f is even and $f(\mathfrak{p}^+/p) = f$ if f is odd.

The same argument shows, upon factoring

$$T(X) = \prod_{\substack{(i,d)=1\\ 0<i<d}} (X - \gamma^i)$$

in $\mathbb{F}_p[X]$, that any prime $\mathfrak{p} \subset \mathcal{O}_K$ over p satisfies $f(\mathfrak{p}/p) = f$. Since $\mathfrak{p}^+$ cannot ramify in $\mathcal{O}_K$ by assumption, the result follows.

Lemma 2.

$$[PU_2(\mathscr{O}_K/\mathfrak{p}) : PSU_2(\mathscr{O}_K/\mathfrak{p})] = \begin{cases} 2, & \textit{if } q \textit{ is odd} \\ 1, & \textit{if } q \textit{ is even}. \end{cases}$$

Proof. We prove the lemma for $\mathscr{O}_K/\mathfrak{p} = \mathbb{F}_{q^2}$; the proof for $\mathscr{O}_K/\mathfrak{p} = \mathbb{F}_q \times \mathbb{F}_q$ is similar.

Note that if $x \in U_2(\mathbb{F}_{q^2})$ and $\det(x) = a$, then $a\bar{a} = a^{q+1} = 1$. Thus the image $\bar{x}$ of x in $PU_2(\mathbb{F}_{q^2})$ is actually in $PSU_2(\mathbb{F}_{q^2})$ if and only if there exists some $\mu \in \mathbb{F}_{q^2}$ with $\mu^2 = a$, $\mu^{q+1} = 1$.

Thus if q is odd, then $\bar{x} \in PSU_2(\mathbb{F}_{q^2}) \Leftrightarrow a^{(q+1)/2} = 1$. So in this case,

$$PU_2(\mathbb{F}_{q^2}) = PSU_2(\mathbb{F}_{q^2}) \cup PSU_2(\mathbb{F}_{q^2})\bar{x},$$

where x is any element of $U_2(\mathbb{F}_{q^2})$ satisfying $\det(x)^{(q+1)/2} = -1$.

If $q = 2^r$ and $a^{q+1} = 1$, set $\mu = a^{q/2+1}$. Then $\mu^2 = a$ and $\mu^{q+1} = 1$. So $PU_2(\mathbb{F}_{q^2}) = PSU_2(\mathbb{F}_{q^2})$.

We thus observe that when we factor through to $PSL_2(\mathbb{Z})$, the worst we can do is surject onto a group in which $PSL_2(\mathbb{F}_q)$ has index 2. We now list the cases in which we land precisely on $PSL_2(\mathbb{F}_q)$.

Proposition 2. *With the notation as above, if* $(p) = \mathfrak{p} \cap \mathbb{Z}$, *then* $PU_2(\zeta, \mathscr{O}_K/\mathfrak{p}) = PSU_2(\mathscr{O}_K/\mathfrak{p})$ *if and only if the following conditions hold*:

Case I. $\mathfrak{p}$ *is prime and* p *is odd.*

(1) $2 \nmid d$: $q \equiv -1 \bmod 4$

(2) $2 \| d$: *always*

(3) $4 \mid d$: $2 \mid (q+1)/d$.

Case II. $\mathfrak{p} = \mathfrak{P}\overline{\mathfrak{P}}$ *and* p *is odd.*

(1) $2 \nmid d$: $q \equiv 1 \bmod 4$

(2) $2 \| d$: *always*

(3) $4 \mid d$: $2 \mid (q-1)/d$.

Case III. $p = 2$: *always*.

Proof. Recall that all elements in $PU_2(\zeta, \mathscr{O}_K/\mathfrak{p})$ have determinant contained in $\langle -\zeta \rangle$.

Case I. We must have $(-\zeta)^{(q+1)/2} + \mathfrak{p} = 1 + \mathfrak{p}$, or equivalently, $(-\zeta)^{(q+1)/2} = 1$. Since $\langle -\zeta \rangle$ has order $2d$, $d/2$, or d depending on whether $2 \nmid d$, $2\|d$, or $4 \mid d$, the result follows.

Case II. Proceed as in Case I.

Assumption. From now on, assume that our map $\pi_{\mathfrak{p}}$ surjects onto $PU_2(\zeta, \mathscr{O}_K/\mathfrak{p}) \cong PSL_2(\mathbb{F}_q)$, that q is odd, and that $(6, k) = 1$, where $k = \#\langle -\zeta \rangle$.

PROPOSITION 3. *$\Gamma(\mathfrak{p})$ is noncongruence.*

Proof. We first quote the following lemma.

LEMMA 3 [W]. *Suppose Δ is a finite index subgroup of $PSL_2(\mathbb{Z})$. Let N denote the least common multiple of the cusp widths of Δ. Then Δ is congruence if and only if $\Delta \supseteq \Gamma(N)$.*

Completion of Proof. Since $\Gamma(\mathfrak{p})$ is normal, all cusp widths will equal $k = \#\langle -\zeta \rangle$. Now if $\Gamma(\mathfrak{p}) \supseteq \Gamma(k)$, then we will have a homomorphism $PSL_2(\mathbb{Z}/k\mathbb{Z}) \to PSL_2(\mathbb{F}_q)$. But this is impossible: Since $q \nmid k$ by assumption, no composition factor of $PSL_2(\mathbb{Z}/k\mathbb{Z})$ could be equal to $PSL_2(\mathbb{F}_q)$.

4. CHARACTER MULTIPLICITIES IN THE REPRESENTATION OF $PSL_2(\mathbb{F}_q)$ ON COHOMOLOGY GROUPS

4.1. *The Calculation on H^1.* We continue our assumption that $PSL_2(\mathbb{Z}/\Gamma(\mathfrak{p}) \cong PSL_2(\mathbb{F}_q)$. Recall that if $k = \#\langle -\zeta \rangle$, then our map $\pi_{\mathfrak{p}}$: $PSL_2(\mathbb{Z}) \to PSL_2(\mathbb{F}_q)$ factors through $T(2,3,k)$ with kernel $\Delta(\mathfrak{p})$. Thus $T(2,3,k)/\Delta(\mathfrak{p}) \cong PSL_2(\mathbb{F}_q)$ as well. Note that for $k > 6$, $T(2,3,k) \hookrightarrow PSU(1,1)$. (We can obtain this injection from the Burau representation as follows: for an appropriate choice of a dth root of unity,

$$H = \begin{bmatrix} 1 & \dfrac{-1}{\zeta + 1} \\ \dfrac{-1}{\zeta^{-1} + 1} & 1 \end{bmatrix}$$

will have negative determinant. Now one may easily verify that the image of B_3 under the Burau representation, evaluation $t \mapsto \zeta$, and reduction mod scalars is isomorphic to $T(2,3,k)$. Thus we have $T(2,3,k)$ embedded as a subgroup of a unitary group which is conjugate to $PSU(1,1)$.) Thus

$T(2,3,k)$ acts on the Poincare disk $\mathbb{D}^1$. Set $R(\mathfrak{p}) = \mathbb{D}^1/\Delta(\mathfrak{p})$ and recall that $\mathbb{D}^1/T(2,3,k) \cong \mathfrak{h}^*/PSL_2(\mathbb{Z}) \cong \mathbb{P}^1$. We thus obtain two isomorphic $PSL_2(\mathbb{F}_q)$ covers of $\mathbb{P}^1$,

$$X(\mathfrak{p}) = \mathfrak{h}^*/\Gamma(\mathfrak{p}) \to \mathfrak{h}^*/PSL_2(\mathbb{Z}) = \mathbb{P}^1$$

and

$$R(\mathfrak{p}) = \mathbb{D}^1/\Delta(\mathfrak{p}) \to \mathbb{D}^1/T(2,3,k) = \mathbb{P}^1.$$

We wish to determine the structures of $H^1(X(\mathfrak{p}),\mathbb{C})$ and $H^{1,0}(X(\mathfrak{p}),\mathbb{C})$ as $\mathbb{C}[PSL_2(\mathbb{F}_q)]$-modules. Observe that the same results hold with $X(\mathfrak{p})$ replaced by $R(\mathfrak{p})$, since the covers are isomorphic.

Now the cover $X(\mathfrak{p}) \to \mathbb{P}^1$ is ramified over the points

$$\begin{gathered} p_2 = PSL_2(\mathbb{Z})e^{2\pi i/4}, \qquad p_3 = PSL_2(\mathbb{Z})e^{2\pi i/6}, \\ \text{and} \qquad p_k = PSL_2(\mathbb{Z})i\infty. \end{gathered} \tag{16}$$

Lying over them are the points

$$P_2 = \Gamma(\mathfrak{p})e^{2\pi i/4}, \qquad P_3 = \Gamma(\mathfrak{p})e^{2\pi i/6}, \qquad \text{and} \qquad P_k = \Gamma(\mathfrak{p})i\infty. \tag{17}$$

Observe that the inertia group of P_2 over p_2 is generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \mod \mathfrak{p},$$

that of P_3 over p_3 by

$$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \mod \mathfrak{p},$$

and that of P_k over p_k by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mod \mathfrak{p}$$

(see subsection 3.1). Call these generators γ_2, γ_3, and γ_k, respectively. (Note that $\gamma_i = \beta_i \bmod \Delta(\mathfrak{p})$.) We can approach $H^1(X(\mathfrak{p}),\mathbb{C})$ by means of the Lefschetz fixed point theorem: for $g \in PSL_2(\mathbb{F}_q)$,

$$\#\mathrm{Fix}(g) = \#(\Delta_{X(\mathfrak{p})} \cdot \Gamma_g) = \sum_{i=0}^{2} (-1)^i \mathrm{tr}(g \mid H^i(X(\mathfrak{p}),\mathbb{C})),$$

where $\Delta_{X(\mathfrak{p})}$ is the diagonal of $X(\mathfrak{p})$ and Γ_g is the graph of g acting on $X(\mathfrak{p})$. We know that $\mathrm{tr}(g \mid H^i(X(\mathfrak{p}),\mathbb{C}) = 1$ for $i = 0, 2$, and we calculate $\#\mathrm{Fix}(g)$ as follows.

Note that our above comments tell us that if g is not conjugate to γ_i, $i = 2, 3, k$, then $\#\mathrm{Fix}(g) = 0$. Furthermore, the only points in $X(\mathfrak{p})$ with nontrivial stabilizers are the points lying over p_2, p_3, p_k. Thus if $\gamma_i x = x$, then since $\gamma_2, \gamma_3, \gamma_k$ all have relatively prime orders, we must have $x = \sigma p_i$ for some $\sigma \in PSL_2(\mathbb{F}_q)$. So

$$\gamma_i \sigma p_i = \sigma p_i \;\Leftrightarrow\; \sigma^{-1}\gamma_i \sigma p_i = p_i \;\Leftrightarrow\; \sigma^{-1}\gamma_i \sigma \in \langle \gamma_i \rangle \;\Leftrightarrow\; \sigma \in N(\langle \gamma_i \rangle).$$

(For a subgroup H of $PSL_2(\mathbb{F}_q)$, $N(H)$ denotes the normalizer of H in $PSL_2(\mathbb{F}_q)$.)

Also,

$$\sigma p_i = \tau p_i \;\Leftrightarrow\; \tau^{-1}\sigma \in \langle \gamma_i \rangle.$$

This implies that

$$\#\mathrm{Fix}(\gamma_i) = \frac{\#N(\langle \gamma_i \rangle)}{\#\langle \gamma_i \rangle}.$$

We now recall the following (see [F-H]):

LEMMA 4. *Any element of $PSL_2(\mathbb{F}_q)$ is conjugate to either*

$$I, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \epsilon \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad \text{or} \quad \begin{pmatrix} x & y\epsilon \\ y & x \end{pmatrix},$$

where $\mathbb{F}_q^* = \langle \epsilon \rangle$.

An element of the fourth type is said to be split Cartan and an element of the fifth type is said to be nonsplit Cartan. The nonsplit Cartan elements form a subgroup of order $(q+1)/2$.

From examining the orders of each conjugacy class, we see that if $2i \mid (q-1)$, then γ_i is conjugate to a split Cartan element, and if $2i \mid (q+1)$, then γ_i is conjugate to a nonsplit Cartan element. Now by [F-H],

$$\#N\langle \gamma \rangle = \begin{cases} q-1, & \gamma \text{ split} \\ q+1, & \gamma \text{ nonsplit}. \end{cases}$$

Also, half the conjugates will equal γ and half will equal γ^{-1}. So

$$\#\mathrm{Fix}(\gamma) = \frac{\#N\langle \gamma \rangle}{\#\langle \gamma \rangle} = \begin{cases} \dfrac{q-1}{i}, & \gamma \sim \gamma_i, \gamma \text{ split} \\[2ex] \dfrac{q+1}{i}, & \gamma \sim \gamma_i, \gamma \text{ nonsplit}. \end{cases}$$

Putting this information together, we obtain the following.

PROPOSITION 4. *If* $\gamma \nsim \gamma_i$, $i = 2, 3, k$, *then* $\operatorname{tr}(\gamma \mid H^1(X(\mathfrak{p}), \mathbb{C})) = 2$. *If* $\gamma \sim \gamma_i$ *for some i as above, then*

$$\operatorname{tr}(\gamma \mid H^1(X(\mathfrak{p}), \mathbb{C})) = \begin{cases} 2 - \dfrac{q-1}{i}, & 2i \mid (q-1) \\ 2 - \dfrac{q+1}{i}, & 2i \mid (q+1). \end{cases}$$

Remark. Our fake congruence groups are generalizations of regular congruence groups, since

$$\begin{pmatrix} -\zeta & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \zeta & -\zeta \end{pmatrix} \qquad \operatorname{mod} p$$

are the usual generators of $SL_2(\mathbb{F}_p)$ when $d = 2$. But in this case, the image $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ of $\sigma_1 \in B_3$ under π_p is unipotent, not Cartan. Thus our subsequent calculations differ in this case.

The list of nontrivial irreducible finite-dimensional representations of $SL_2(\mathbb{F}_q)$ is quite short (see [F-H]):

(1) The complement V of Σg in the permutation representation is irreducible.

(2) Let $B = \{\left(\begin{smallmatrix} a & b \\ 0 & a^{-1} \end{smallmatrix}\right)\}$ be the Borel subgroup of $PSL_2(\mathbb{F}_q)$. Suppose $\mathbb{F}_q^* = \langle \epsilon \rangle$ and $\rho = e^{2\pi i/(q-1)}$. The map

$$\begin{pmatrix} \epsilon^n & * \\ 0 & \epsilon^{-n} \end{pmatrix} \to \rho^n$$

gives a 1-dimensional representation W_n of B; $\operatorname{Ind}_B^{PSL_2(\mathbb{F}_q)} W_n =: Y_n$ is irreducible if $n \neq (q-1)/2$; and for $n = (q-1)/2$, Y_n splits into two irreducible factors Y^+ and Y^-.

(3) If C denotes the nonsplit Cartan subgroup $\{\left(\begin{smallmatrix} x & y\epsilon \\ y & x \end{smallmatrix}\right)\}$ and

$$\phi_m \colon C \to \mathbb{C}$$

is a character, then $V \otimes Y_m \equiv \operatorname{Ind}_C^{PSL_2(\mathbb{F}_q)} \phi \oplus Y_m \oplus Z_m$ for some representation Z_m which is irreducible if $m \neq (q = 1)/2$ and splits into two irreducible factors Z^+ and Z^- otherwise.

We would like to know the multiplicity of each irreducible representation in our representation $\rho_{\mathfrak{p}} \colon PSL_2(\mathbb{F}_q) \to \operatorname{Aut}(H^1(X(\mathfrak{p}), \mathbb{C}))$. We may use the standard character formula $m_\chi = \sum_{\sigma \in PSL_2(\mathbb{F}_q)} \chi_{\mathfrak{p}}(\gamma)\overline{\chi(\gamma)}$, where $\chi_{\mathfrak{p}}$ is the character of $\rho_{\mathfrak{p}}$ and χ is irreducible.

TABLE I
Character Multiplicities

V	$q - \sum_{i} a_i - T$
Y_{2r}	$q + 1 - T - \sum_{\substack{i \\ i \mid r}} (a_i + 1)$
Z_{2m}	$q - 1 - T - \sum_{\substack{i \\ i \bmod m}} (1 - a_i)$
Y^+, Y^-	$\frac{q+1}{2} - \frac{1}{2} T - \sum_{\substack{a_i = 1 \\ \frac{q+1}{2i} \text{ even}}} 1$
Z^+, Z^-	$\frac{q-1}{2} - \frac{1}{2} T - \sum_{\substack{a_i = -1 \\ \frac{q+1}{2i} \text{ even}}} 1$

THEOREM 6. *Assumptions as above, define $a_i \in \langle \pm 1 \rangle$ by $q \equiv a_i \bmod i$ for $i = 2, 3, k$. Also, let*

$$T = \sum_{i = 2, 3, 7} \frac{q - a_i}{i}.$$

Then the character multiplicities are as listed in Table I, *where i runs through $2, 3, k$, Y^+ and Y^- appear only for $q \equiv 1 \bmod 4$, and Z^+ and Z^- appear only for $q \equiv -1 \bmod 4$.*

Proof. We make use of the character table of [F-H]. We note that representations of $PSL_2(\mathbb{F}_q)$ are the same as representations of $SL_2(\mathbb{F}_q)$ that map -1_2 to the identity. In the representation V, the character of $\pm 1_2$ is q, the character of a split (respectively, nonsplit) Cartan element is 1 (respectively, -1), and there are $(q-3)/2$ (respectively, $(q-1)/2$) conjugacy classes with $q^2 + q$ (respectively, $q^2 - q$) elements in each class. Our multiplicity then becomes

$$\frac{1}{\#PSL_2(\mathbb{F}_q)} \cdot \Bigg(4qg + (q^2 + q) \cdot \left[2\left(\frac{q-3}{2} - \sum X_i \right) + \sum \left(2 - \frac{q-1}{i} \right) X_i \right] - (q^2 - q) \cdot \left[2\left(\frac{q-1}{2} - \sum Y_i \right) + \sum \left(2 - \frac{q+1}{i} \right) Y_i \right] \Bigg).$$

Here, X_i (respectively, Y_i) is the number of conjugacy classes of elements in the cyclic subgroup $\langle \gamma_i \rangle$ that are split (nonsplit) Cartan. Thus,

$$X_i = \begin{cases} i-1, & a_i = 1 \\ 0, & a_i = -1 \end{cases}$$

and $Y_i = d - 1 - X_i$. Summing up gives us the desired result.

Further use of the character tables gives us the following.

The multiplicity for Y_{2r} is

$$\frac{1}{\#PSL_2(\mathbb{F}_q)} \cdot \Bigl(4(q+1)g + 4(q^2-1) + (q^2+q) \\ \cdot \Bigl[2\bigl(-2 - \sum A_i\bigr) + \sum \Bigl(2 - \frac{q-1}{i}\Bigr) A_i\Bigr]\Bigr),$$

where

$$A_i = \begin{cases} 0, & a_i = -1 \\ -2, & a_i = 1, i \nmid r \\ -2 + 2i, & a_i = 1, i \mid r. \end{cases}$$

The multiplicity for Z_{2m} is

$$\frac{1}{\#PSL_2(\mathbb{F}_q)} \cdot \Bigl(4(q-1)g - 4(q^2-1) \\ + (q^2-q) \cdot \Bigl[2\bigl(2 - \sum B_i\bigr) + \sum \Bigl(2 - \frac{q-1}{i}\Bigr) B_i\Bigr]\Bigr),$$

where

$$B_i + \begin{cases} 0, & a_i = 1 \\ 2, & a_i = -1, i \nmid m \\ 2 - 2i, & a_i = -1, i \mid m. \end{cases}$$

The multiplications for Y^+ and Y^- are

$$\frac{1}{\#PSL_2(\mathbb{F}_q)} \cdot \Bigg(2(q+1)g + 2(q^2-1) \\ + (q^2+q) \cdot \Bigg[2\Big(-1 - \sum C_i\Big) + \sum \Big(2 - \frac{q-1}{i}\Big) C_i\Bigg]\Bigg),$$

where

$$C_i = \begin{cases} 0, & a_i = -1 \\ -1+i, & a_i = 1,\ \dfrac{q-1}{2i} \text{ even} \\ -1, & a_i = 1,\ \dfrac{q-1}{2i} \text{ odd.} \end{cases}$$

The multiplicities for Z^+ and Z^- are

$$\frac{1}{\#PSL_2(\mathbb{F}_q)} \cdot \Bigg(2(q-1)g - 2(q^2-1) \\ + (q^2-q) \cdot \Bigg[2\Big(1 - \sum D_i\Big) + \sum \Big(2 - \frac{q+1}{i}\Big) D_i\Bigg]\Bigg),$$

where

$$D_i = \begin{cases} 0, & a_i = 1 \\ 1-i, & a_i = -1,\ \dfrac{q+1}{2i} \text{ even} \\ 1, & a_i = 1,\ \dfrac{q+1}{2i} \text{ odd.} \end{cases}$$

Again, summing up gives us the desired results.

4.2. *The Calculation on* $H^{1,0}$. Note that if $g \in PSL_2(\mathbb{F}_q)$, $p \in X(\mathfrak{p})$, and $g(p) = p$, then g induces an automorphism

$$g_{*,p}: T_{X(\mathfrak{p}),p} \to T_{X(\mathfrak{p}),p}$$

of the tangent space of $X(\mathfrak{p})$ at p. Since $T_{X(\mathfrak{p}),p}$ is 1-dimensional, $g_{*,p} = e^{i\theta}$ for some $\theta \in \mathbb{R}$. We can calculate $e^{i\theta}$ as follows: choose $\tilde{g} \in PSL_2(\mathbb{Z})$

such that $\Gamma(\mathfrak{p})\tilde{g} = g$ and $z_p \in \mathfrak{h}^*$ such that $\Gamma(\mathfrak{p})z_p = p$. Then in local coordinates,

$$g_{*,p}\frac{\partial}{\partial z} = \tilde{g}'(z_p)\frac{\partial}{\partial z},$$

and so if $\tilde{g} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then

$$g_{*,p} = \frac{1}{\left(cz_p + d\right)^2}.$$

So choose

$$\tilde{\gamma}_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \tilde{\gamma}_3 = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \qquad \text{and} \qquad \tilde{\gamma}_k = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Let $z_2 = e^{2\pi i/4}$, $z_3 = e^{2\pi i/6}$, and $z_k = i\infty$. Then one may easily check that $\gamma_{j*,p_j} = e^{2\pi i/j}$ for $j = 2, 3$. For $j = k$, use the transformation $z \mapsto e^{2\pi i z/k}$. In these coordinates, $z \mapsto \tilde{\gamma}_k z = z + 1$ becomes the map $y \mapsto e^{2\pi i/k}y$. Thus $\gamma_{k*,p_k} = e^{2\pi i/k}$ as well.

Noting that

$$\begin{tikzcd} X(\mathfrak{p}) \arrow[r, "g"] \arrow[d, "\sigma"'] & X(\mathfrak{p}) \arrow[d, "\sigma^{-1}"] \\ X(\mathfrak{p}) \arrow[r, "\sigma g \sigma^{-1}"] & X(\mathfrak{p}) \end{tikzcd}$$

induces an equality $g_{*,\sigma p} = (\sigma^{-1} g \sigma)_{*,p}$, we see that

$$\gamma_{j*,\sigma p_j} = \begin{cases} e^{2\pi i/j}, & \sigma^{-1}\gamma_j\sigma = \gamma_j \\ e^{-2\pi i/j}, & \sigma^{-1}\gamma_j\sigma = \gamma_j^{-1}. \end{cases}$$

Now we make use of the following:

THEOREM 7 (Holomorphic Lefschetz Fixed Point Theorem). *Let*

$$Lef\left(g, \mathcal{O}_{X(\mathfrak{p})}\right) = \sum_{\substack{p \in Fix(g) \\ g_{*,p} = e^{i\theta}}} \frac{1}{1 - e^{-i\theta}}.$$

Then

$$Lef\left(g, \mathcal{O}_{X(\mathfrak{p})}\right) = \sum_{i=0}^{\infty} (-1)^i \operatorname{tr}\left(g^* \mid H^{i,0}(X(\mathfrak{p}), \mathbb{C})\right).$$

THEOREM 8. *Let* $\rho_{\mathfrak{p}}^{1,0}$ *denote the representation* $g \to \mathrm{Aut}(H^{1,0}(X(\mathfrak{p}), \mathbb{C}))$. *Then* $\chi_{\mathfrak{p}}^{1,0} = \frac{1}{2}\chi_{\mathfrak{p}}$.

Note. This differs sharply from the congruence case.

Proof. From our above calculations, we see that for any $\alpha \in PSL_2(\mathbb{F}_q)$,

$$Lef\left(\gamma_j^{\alpha}, \mathscr{O}_{X(\mathfrak{p})}\right) = \frac{q \pm 1}{2j}\left(\frac{1}{1 - e^{-\pi i/j}} + \frac{1}{1 + e^{-\pi i/j}}\right) = \frac{q \pm 1}{2j} \qquad (18)$$

$$= \frac{1}{2}\#\mathrm{Fix}\left(\gamma_j^{\alpha}\right), \qquad (19)$$

since $\sigma^{-1}\gamma_j\sigma = \gamma_j$ or γ_j^{-1} for $q \pm 1/2j$ elements σ modulo $\langle \gamma_j \rangle$.

Then by the holomorphic Lefschetz fixed point theorem,

$$\mathrm{tr}\left(\gamma^* \mid H^{1,0}(X(\mathfrak{p}), \mathbb{C})\right) = 1 - \mathrm{Lef}(\gamma, 'X(\mathfrak{p})) \qquad (20)$$

$$= 1 - \frac{1}{2}\#\mathrm{Fix}(\gamma) = \frac{1}{2}\chi_{\mathfrak{p}}(\gamma) \qquad \forall\gamma. \quad (21)$$

5. GENERA OF QUOTIENT CURVES

5.1. *The Calculation.* Let $J(\mathfrak{p})$ denote the Jacobian of $X(\mathfrak{p})$. We would like to understand the decomposition of $J(\mathfrak{p})$ into simple factors. As a first step in this direction, we calculate the genera of certain quotient curves of $X(\mathfrak{p})$.

Suppose L is a subgroup of $\mathbb{F}_q^*$ with $[\mathbb{F}_q^*/\langle \pm 1\rangle \colon \pm L/\langle \pm 1\rangle] = \alpha_L$. Define a subgroup B_L of $PSL_2(\mathbb{F}_q)$ by

$$B_L = \left\{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \in L\right\}.$$

Let C be the nonsplit Cartan subgroup of $PSL_2(\mathbb{F}_q)$ and S be the split Cartan subgroup $\{\left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right)\}$. Denote the genus of $X(\mathfrak{p})/H$ by $g(H)$ for any subgroup of $PSL_2(\mathbb{F}_q)$.

PROPOSITION 5. *We have the following*:

(1) $2g(\{1\}) - 2 = \#PSL_2(\mathbb{F}_q)(1 - \sum_i(1/i))$

(2) $2g(B_L) - 2 = \alpha_L(q + 1 - \sum_i \epsilon_i)$

(3) $2g(C) - 2 = q(q - 1) - \sum_i \delta_i$

(4) $2g(S) - 2 = q(q + 1) - \sum_i \gamma_i$,

where all summations are over $i = 2, 3, k$ *and*

$$\epsilon_i \ (\textit{resp.}, \ \delta_i, \gamma_i) = \begin{cases} \dfrac{q-1}{i} + 2 & \left(\textit{resp.}, \dfrac{q(q-1)}{i}, \dfrac{(q-1)(q+2)}{i} + 2\right), q \equiv 1(i) \\ \dfrac{q+1}{i} & \left(\textit{resp.}, \dfrac{(q+1)(q-2)}{i} + 2, \dfrac{q(q+1)}{i}\right), q \equiv -1(i). \end{cases}$$

Proof. Let H be any subgroup of $PSL_2(\mathbb{F}_q)$, and let p_i, γ_i, be as in Section 4. Using the Hurwitz formula,

$$\begin{aligned} 2g(H) - 2 &= \left[PSL_2(\mathbb{F}_q) \colon H\right] \cdot (-2) \\ &\quad + \sum_i \left(\left[PSL_2(\mathbb{F}_q) \colon H\right] - \#\text{ points over } p_i\right) \qquad (22) \\ &= \left[PSL_2(\mathbb{F}_q) \colon H\right] - \sum_i \#\text{points over } p_i. \qquad (23) \end{aligned}$$

Now if $PSL_2(\mathbb{F}_q) = \cup H\beta_j$, the ramification index of $\beta_j p_i$ over p_i is

$$\left[\langle \gamma_i^{\beta_j} \rangle \colon \langle \gamma_i^{\beta_j} \rangle \cap H\right].$$

We calculate these indices in the case $H = B_L$; the remaining cases are similar.

First, note that a set of coset representatives for B_L in $PSL_2(\mathbb{F}_q)$ is given by

$$\left\{ \begin{pmatrix} a & 0 \\ a^{-1}t & a^{-1} \end{pmatrix} = A_{a,t}, \begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix} \right\},$$

where a runs over a set of coset representatives for L in $\mathbb{F}_q^*$ and t is an arbitrary element of $\mathbb{F}_q$. We may assume by Lemma 5 that γ_i is split or nonsplit Cartan; we will examine these cases separately. So assume that γ_i is split, and hence of the form $\left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right)$. Then

$$A_{a,t} \cdot \gamma_i \cdot A_{a,t}^{-1} = \begin{pmatrix} x & 0 \\ a^{-2}t(x - x^{-1}) & x^{-1} \end{pmatrix}.$$

We thus see that $\langle \gamma_i \rangle^{A_{a,t}} \cap B_L$ is trivial unless $t = 0$, in which case $\langle \gamma_i \rangle^{A_{a,t}} \subseteq B_L$.

Also,

$$\begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix} = \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix}.$$

Hence in this case, the index in question will always be 1.

So in $2\alpha_L$ cases our index is 1, and in $[PSL_2(\mathbb{F}_q)\colon\ B_L] - 2\alpha_L = (q-1)\alpha_L$ cases, our index is i. Thus we have $2\alpha_L$ unramified points and $(q-1)\alpha_L/i$ points with ramification index i. Our proposition then follows in this case.

Now assume that γ_i is nonsplit, and hence of the form $\left(\begin{smallmatrix} x & y \\ y\epsilon & x \end{smallmatrix}\right)$. Then

$$A_{a,t} \cdot \gamma_i \cdot A_{a,t}^{-1} = \begin{pmatrix} x - yt & a^2 y \\ a^{-2} y(\epsilon - t^2) & x + yt \end{pmatrix}.$$

We thus see that $\langle \gamma_i \rangle^{A_{a,t}} \cap B_L$ is always trivial, since y is never 0 (as the order of γ_i is i) and ϵ cannot be a square.

Also,

$$\begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix} \begin{pmatrix} x & y \\ y\epsilon & x \end{pmatrix} \begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix} = \begin{pmatrix} x & -a^2 y\epsilon \\ -a^{-2} y & x \end{pmatrix}.$$

Thus in all $(q+1)\alpha_L$ cases the ramification index is i, and we thus obtain $(q+1)\alpha_L/i$ points in this case. This completes the proof of the proposition for B_L.

5.2. AN EXAMPLE. Suppose $d = 14$, and choose $\zeta = -e^{2\pi i/7}$. As usual, set $F = \mathbb{Q}(\zeta + \zeta^{-1})$ and $K = \mathbb{Q}(\zeta)$. Let $\mathfrak{p}^+ = (13, \zeta + \zeta^{-1} + 7) \subset \mathscr{O}_F$. Then one may verify that $\mathfrak{p}^+$ remains prime in $\mathscr{O}_K$, that $\mathscr{O}_F/\mathfrak{p}^+ = \mathbb{Z}/(13)$, and that the map $X \mapsto -\zeta$ induces an isomorphism

$$\mathbb{Z}[X]/(13, X^2 - 7X + 1) \cong \mathscr{O}_K/\mathfrak{p}^+\mathscr{O}_K.$$

Let $\epsilon = X + 3 \bmod (13, X^2 - 7X + 1)$. Then $\epsilon^2 = x^2 + 6X + 9$, which equals 8 mod $(13, X^2 - 7X + 1)$. Now conjugation in $\mathbb{Z}[X]/(13, X^2 - 7X + 1)$ is given by

$$\begin{aligned} X \bmod (13, X^2 - 7X + 1) &\mapsto X^{-1} \bmod (13, X^2 - 7X + 1) \\ &= 7 - X \bmod (13, X^2 - 7X + 1). \end{aligned}$$

So $\bar{\epsilon}$ is equal to $(7 - X) + 3 \bmod(13, X^2 - 7X + 1)$, which is just $-\epsilon$.

Recall that our map $\pi\colon PSL_2(\mathbb{Z}) \to PSU(\zeta, H, \mathbb{F}_{13^2})$ is given by

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} \epsilon - 3 & 1 \\ 0 & 1 \end{pmatrix} \tag{24}$$

$$U = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ -\epsilon + 3 & \epsilon - 3 \end{pmatrix}. \tag{25}$$

since $\epsilon - 3 = X \bmod(13, X^2 - 7X + 1)$ corresponds to $-\zeta$ under our isomorphism.

Now conjugate each matrix by

$$\begin{pmatrix} 6\epsilon + 1 & 7\epsilon + 2 \\ 0 & 4 \end{pmatrix}$$

and multiply by $9\epsilon + 5$. (The latter is permitted since we're working mod scalars.) Then

$$\begin{pmatrix} \epsilon - 3 & 1 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 5 + 4\epsilon & 0 \\ 0 & 5 - 4\epsilon \end{pmatrix} \tag{26}$$

$$\begin{pmatrix} 1 & 0 \\ -\epsilon + 3 & \epsilon - 3 \end{pmatrix} \mapsto \begin{pmatrix} 5 - 3\epsilon & 6 + 2\epsilon \\ 6 - 2\epsilon & 5 + 3\epsilon \end{pmatrix}, \tag{27}$$

and we thus obtain generators for $PSU_2(\mathbb{F}_{13^2})$. Under the canonical isomorphism $PSU_2(\mathbb{F}_{13^2}) \to PSL_2(\mathbb{F}_{13})$ given by

$$\begin{pmatrix} a + b\epsilon & c + d\epsilon \\ c - d\epsilon & a - b\epsilon \end{pmatrix} \mapsto \begin{pmatrix} a + c & \epsilon^2(b - d) \\ b + d & a - c \end{pmatrix},$$

we observe that

$$\begin{pmatrix} 5 + 4\epsilon & 0 \\ 0 & 5 - 4\epsilon \end{pmatrix} \mapsto \begin{pmatrix} 5 & 6 \\ 4 & 5 \end{pmatrix} \tag{28}$$

$$\begin{pmatrix} 5 - 3\epsilon & 6 + 2\epsilon \\ 6 - 2\epsilon & 5 + 3\epsilon \end{pmatrix} \mapsto \begin{pmatrix} -2 & -1 \\ -1 & -1 \end{pmatrix}. \tag{29}$$

Our composite map is then

$$\Omega\colon PSL_2(\mathbb{Z}) \to PSL_2(\mathbb{F}_{13})\colon \tag{30}$$

$$S \mapsto \begin{pmatrix} 5 & 6 \\ 4 & 5 \end{pmatrix} \tag{31}$$

$$U \mapsto \begin{pmatrix} -2 & -1 \\ -1 & -1 \end{pmatrix}. \tag{32}$$

Setting $\gamma_2 = \Omega(USU)$, $\gamma_3 = \Omega(SU)$, and $\gamma_7 = \Omega(S)$, we finally obtain the following images of the generators of $T(2,3,7)$:

$$\gamma_2 = \begin{pmatrix} 7 & 8 \\ 10 & 6 \end{pmatrix}, \qquad \gamma_3 = \begin{pmatrix} 9 & 2 \\ 0 & 3 \end{pmatrix}, \qquad \gamma_7 = \begin{pmatrix} 5 & 6 \\ 4 & 5 \end{pmatrix}.$$

Using our genus formulas, we see that our associated curve has genus 14, and that the representation into $\mathrm{Aut}(H^1(R_{\mathscr{N}}, \mathbb{C}))$ is just $Y_2 \oplus Y_2$.

REFERENCES

[A-Sw] O. Atkin and H. P. F. Swinnerton-Dyer, Modular forms on noncongruence subgroups, *in* Proc. Sympos. Pure Math., Vol. 19, pp. 1–25, Amer. Math. Soc., Providence, 1971.

[Be] G. V. Belyi, On extensions of the maximal cyclotomic field having a given Galois group, *J. Reine. Angew. Math.* **341** (1983), 1–25.

[B] G. Berger, Hecke operators on non-congruence subgroups, *C. R. Acad. Sci. Paris Sér. I. Math.* **319** (1994), 915–919.

[B2] G. Berger, Fake congruence subgroups and the Hurwitz monodromy group, draft, 1997.

[B-F] G. Berger and M. Fried, The Hurwitz monodromy group H_4, in preparation, 1997.

[C] H. Cohen, ‘‘A Course in Computational Algebraic Number Theory,’’ Grad. Texts in Math., Vol. 138, Springer-Verlag, New York/Berlin, 1993.

[Bi] J. Birman, Braids, links, and mapping class groups, Princeton, 1973.

[F] M. Fried, Arithmetic of 3 and 4 branch point covers: A bridge provided by noncongruence subgroups of $SL(2, Z)$, *in* ‘‘Sem. de Theorie des Nombres, Paris, 1987-88,’’ Prog. Math., Vol. 81, pp. 77–117, Birkhäuser, Basel, 1990.

[F-V] M. Fried and H. Volklein, The inverse Galois problem and rational points on moduli spaces, *Math. Ann.* **290**, No. 4 (1991), 771–800.

[F2] M. Fried, Introduction to modular towers: Generalizing dihedral group-modular curve connections, *in* ‘‘Recent Developments in the Inverse Galois Problem,’’ Contemporary Mathematics, Vol. 186, pp. 111–173, Amer. Math. Soc., Providence, 1995.

[F-H] W. Fulton and J. Harris, ‘‘Representation Theory: A First Course,’’ Springer-Verlag, New York, 1991.

[M] A. M. Macbeath, Generators of the linear fractional groups, *in* Proc. Sympos. Pure Math., Vol. 12, pp. 14–32, Amer. Math. Soc., Providence, 1968.

[O-T] T. Oda and T. Terasoma, Surjectivity of reductions of the Burau representation of Artin braid groups, draft, 1995.

[Sch] A. J. Scholl, Modular forms and de Rham cohomology; Atkin−Swinnerton−Dyer congruences, *Invent. Math.* **79** (1985), 49−77.

[V] H. Volklein, Braid group action via $GL(n, q)$ and $U(n, q)$, and Galois realizations, *Israel J. Math.* **82** (1993), 405−427.

[W] K. Wolfahrt, An extension of F. Klein's level concept, *Internat. J. Math.* **8** (1967), 529−535.