CONGRUENCE SUBGROUPS AND SUPER-MODULAR CATEGORIES

PARSA BONDERSON, ERIC C. ROWELL, ZHENGHAN WANG, AND QING ZHANG

Abstract. A super-modular category is a unitary pre-modular category with Müger center equivalent to the symmetric unitary category of super-vector spaces. Super-modular categories are important alternatives to modular categories as any unitary pre-modular category is the equivariantization of either a modular or super-modular category. Physically, super-modular categories describe universal properties of quasiparticles in fermionic topological phases of matter. In general one does not have a representation of the modular group $\text{SL}(2, \mathbb{Z})$ associated to a super-modular category, but it is possible to obtain a representation of the (index 3) $\theta$-subgroup: $\Gamma_\theta < \text{SL}(2, \mathbb{Z})$. We study the image of this representation and conjecture a super-modular analogue of the Ng-Schauenburg Congruence Subgroup Theorem for modular categories, namely that the kernel of the $\Gamma_\theta$ representation is a congruence subgroup. We prove this conjecture for any super-modular category that is a subcategory of modular category of twice its dimension, i.e. admitting a minimal modular extension. Conjecturally, every super-modular category admits (precisely 16) minimal modular extensions and, therefore, our conjecture would be a consequence.

E. Rowell and Q. Zhang were partially supported by NSF grant DMS-1410144, and Z. Wang by NSF grant DMS-1411212. The authors thank M. Cheng, M. Papanikolas and Z. Sunic for valuable discussions.

1. Introduction

A key part of the data for a modular category $\mathcal{C}$ is the $S$ and $T$ matrices encoding the non-degeneracy of the braiding and the twist coefficients, respectively. We will denote by $\tilde{S}$ the unnormalized matrix obtained as the invariants of the Hopf link so that $\tilde{S}_{0,0} = 1$, while $S = \frac{\tilde{S}}{D}$ will denote the (unitary) normalized $S$-matrix where $D^2 = \text{dim}(\mathcal{C})$ is the categorical dimension and $D > 0$. Later, we will use the same conventions for any pre-modular category (for which $S$ may not be invertible). The diagonal matrix $T := \theta \delta_{i,j}$ has finite order (Vafa’s theorem, see [2]) for any pre-modular category. For a modular category the $S$ and $T$ matrices satisfy (see e.g. [2, Theorem 3.1.7]):

1. $S^2 = C$ where $C_{i,j} = \delta_{i,j}$, (so $S^4 = C^2 = I$)
2. $(ST)^3 = \frac{D}{D^2} S^2$ where $D = \sum_i \tilde{S}^2_{0,i} \theta_i$
3. $TC = CT$.

These imply that from any modular category $\mathcal{C}$ of rank $r$ (i.e. with $r$ isomorphism classes of simple objects) one obtains a projective unitary representation of the modular group $\rho : \text{SL}(2, \mathbb{Z}) \to \text{PSU}(r)$ defined on generators by: $s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \to S$ and $t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \to T$ composed with the canonical projection $\pi_r : U(r) \to \text{PSU}(r)$. By rescaling the $S$ and $T$ matrices, $\rho$ may be lifted to a linear representation of $\text{SL}(2, \mathbb{Z})$, but these lifts are not unique. This representation has topological significance: one identifies the modular group with the mapping class group $\text{Mod}(\Sigma_{1,0})$ of the torus ($t$ and $st^{-1}s^{-1}$ correspond to Dehn twists about the meridian and parallel) and this projective
representation is the action of the mapping class group on the Hilbert space associated to the torus by the modular functor obtained from $C$.

A subgroup $H < SL(2, \mathbb{Z})$ is called a **congruence subgroup** if $H$ contains a principal congruence subgroup $\Gamma(n) := \{ A \in SL(2, \mathbb{Z}) : A \equiv I \pmod{n} \}$ for some $n \geq 1$. Since $\Gamma(n)$ is the kernel of the reduction modulo $n$ map $SL(2, \mathbb{Z}) \to SL(2, \mathbb{Z}/n\mathbb{Z})$, any congruence subgroup has finite index. The **level** of a congruence subgroup $H$ is the minimal $n$ so that $\Gamma(n) < H$. More generally, for $G < SL(2, \mathbb{Z})$ we say $H < G$ is a congruence subgroup if $G \cap \Gamma(n) < H$ with the level of $H$ defined similarly.

The connection between topology and number theory found through the representation above is deepened by the following Congruence Subgroup Theorem:

**Theorem 1.1** ([25]). Let $C$ be a modular category of rank $r$ with $T$ matrix of order $N$. Then the projective representation $\rho : SL(2, \mathbb{Z}) \to PSU(r)$ has $\ker(\rho)$ a congruence subgroup of level $N$.

In particular the image of $\rho$ factors over $SL(2, \mathbb{Z}/N\mathbb{Z})$ and hence is a finite group. This fact has many important consequences: for example, it is related to rank-finiteness [13] and can be used in classification problems [14].

A **super-modular** category is a unitary ribbon fusion category whose Müger center is equivalent, as a unitary symmetric ribbon fusion category, to the category $sVec$ of super-vector spaces (equipped with its unique structure as a unitary spherical symmetric fusion category). Super-modular categories (or slight variations) have been studied from several perspectives, see [7, 15, 12, 8, 22] for a few examples. An algebraic motivation for studying these categories is the following: any unitary braided fusion category is the equivariantization [18] of either a modular or super-modular category (see [28, Theorem 2]). Physically, super-modular categories provide a framework for studying fermionic topological phases of matter [12]. Topological motivations include the study of spin 3-manifold invariants ([28, 5, 6]) and (3 + 1)-TQFTs ([29]).

**Remark 1.** We restrict to unitary categories both for mathematical convenience and for their physical significance. On the other hand, there is a non-unitary version $sVec^{-}$ of $sVec$: the underlying (non-Tannakian) symmetric fusion category is the same, but with the other possible spherical structure, which leads to negative dimensions. We could define super-modular categories more generally as pre-modular categories $B$ with Müger center equivalent to either of $sVec$ or $sVec^{-}$. However, we do not know of any examples $B$ with $B' \cong sVec^{-}$ that are not simply of the form $C \boxtimes sVec^{-}$ for some modular category $C$ (A. Bruguières asked the second and third authors for such an example in 2016).

One interesting feature of super-modular categories $B$ is that their $S$ and $T$ matrices have tensor decompositions ([9, Appendix], [12, Theorem III.5]):

$$S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \hat{S}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \hat{T}$$ (1.1)

where $\hat{S}$ is unitary and $\hat{T}$ is a diagonal (unitary) matrix, depending on $r/2 - 1$ sign choices. Two naive questions motivated by the above are: 1) Do $\hat{S}$ and a choice of $\hat{T}$ provide a (projective) representation of $SL(2, \mathbb{Z})$? and 2) Is the group generated by $\hat{S}$ and a choice of $\hat{T}$ finite? Of course if $B = sVec \boxtimes D$ for some modular category $D$ (split super-modular) then the answer to both is yes. More generally, as Example 2.1 below illustrates, the answer to both questions is no.

The physical and topological applications of super-modular categories motivate a more refined question as follows. The consideration of fermions on a torus [1] leads to the study of spin structures on...
the torus $\Sigma_{1,0}$: there are three even spin structures $(A,A), (A,P), (P,A)$ and one odd spin structure $(P,P)$, where $A,P$ denote antiperiodic and periodic boundary conditions. The full mapping class group $\text{Mod}(\Sigma_{1,0}) = \text{SL}(2,\mathbb{Z})$ permutes the even spin structures: $s$ interchanges $(P,A)$ and $(A,P)$, and preserves $(A,A)$, whereas $t$ interchanges $(A,A)$ and $(P,A)$ and preserves $(A,P)$. Note that both $s$ and $t^2$ preserve $(A,A)$, so that the index 3 subgroup $\Gamma_0 := \langle s, t^2 \rangle \leq \text{SL}(2,\mathbb{Z})$ is the spin mapping class group of the torus equipped with spin structure $(A,A)$. The spin mapping class group of the torus with spin structure $(A,P)$ or $(P,A)$ is similarly generated by $s^2$ and $t$, which is projectively isomorphic to $\mathbb{Z}$. On the other hand, $\Gamma_0$ is projectively the free product of $\mathbb{Z}/2\mathbb{Z}$ with $\mathbb{Z}$ ($\langle 2 \rangle$). Now the matrix $\hat{T}^2$ is unambiguously defined for any super-modular category $\mathcal{B}$, and in [12, Theorem II.7] it is shown that $\mathfrak{s} \to \hat{S}$ and $t^2 \to \hat{T}^2$ defines a projective representation $\hat{\rho}$ of $\Gamma_0$.

We propose the following:

**Conjecture 1.1.** Let $\mathcal{B}$ be a super-modular category of rank $2k$ and $\hat{S}$ and $\hat{T}^2$ the corresponding matrices as in equation (1.1). Then the projective representation $\hat{\rho} : \Gamma_0 \to \text{PSU}(k)$ given by $\hat{\rho}(s) = \pi_k(\hat{S})$ and $\hat{\rho}(t^2) = \pi_k(\hat{T}^2)$ has kernel a congruence subgroup.

In particular if this conjecture holds then $\hat{\rho}(\Gamma_0)$ is finite. We do not know what to expect the level of $\ker \hat{\rho}$ to be (in terms of, say, the order of $\hat{T}^2$), but we provide some examples below.

An important outstanding conjecture ([16, Question 5.15], [12, Conjecture III.9], see also [23, Conjecture 5.2]) is that every super-modular category $\mathcal{B}$ has a minimal modular extension: that is, $\mathcal{B}$ can be embedded in a modular category $\mathcal{C}$ of dimension $\dim(\mathcal{C}) = 2 \dim(\mathcal{B})$. One may characterize such $\mathcal{C}$: they are called spin modular categories ([3]), see Section 5.1 below. Our main result proves Conjecture 1.1 for super-modular categories admitting minimal modular extensions.

## 2. Preliminaries

### 2.1. Super-Modular Categories

Whereas one may always define an $S$-matrix for any ribbon fusion category $\mathcal{B}$, it may be degenerate. This failure of modularity is encoded it the subcategory of transparent objects called the Müger center $\mathcal{B}'$. Here an object $X$ is called transparent if all the double braidings with $X$ are trivial: $c_{Y,X}c_{X,Y} = Id_{X\otimes Y}$. By a theorem of Bruguières ([11]), the simple objects in $\mathcal{B}'$ are those $X$ with $\hat{S}_{X,Y} = d_Xd_Y$ for all simple $Y$, where $d_Y = \dim(Y) = \hat{S}_{1,Y}$ is the categorical dimension of the object $Y$. The Müger center is obviously symmetric, that is, $c_{Y,X}c_{X,Y} = Id_{X\otimes Y}$ for all $X,Y \in \mathcal{B}'$. Symmetric fusion categories have been classified by Deligne ([17]), in terms of representations of supergroups. In the case that $\mathcal{B}' \cong \text{Rep}(G)$ (i.e. is Tannakian), the modularization (de-equivariantization) procedure of Bruguières ([11]) and Müger ([24]) yields a modular category $\mathcal{B}_G$ of dimension $\dim(\mathcal{B})/[G]$. Otherwise, by taking a maximal Tannakian subcategory $\text{Rep}(G) \subset \mathcal{B}'$ the de-equivariantization $\mathcal{B}_G$ has Müger center $(\mathcal{B}_G)' \cong s\text{Vec}$, the symmetric fusion category of super-vector spaces. Generally, a braided fusion category $\mathcal{B}$ with $\mathcal{B}' \cong s\text{Vec}$ as symmetric fusion categories is called slightly degenerate ([18]).

The symmetric fusion category $s\text{Vec}$ has a unique spherical structure compatible with unitarity and has $S$– and $T$–matrices: $S_{s\text{Vec}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ and $T_{s\text{Vec}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

From this point on we will assume that all our categories are unitary, so that $s\text{Vec}$ is a unitary symmetric fusion category. A unitary slightly degenerate ribbon category will be called super-modular. In other terminology, we say $\mathcal{B}$ is super-modular if its Müger center is generated by a fermion, that is, an object $\psi$ with $\psi^\otimes 2 \cong 1$ and $\theta_\psi = -1$. 


Equation (1.1) shows that the $S$ and $T$ matrices of any super-modular category can be expressed as (Kronecker) tensor products: $S = S_{\text{Vec}} \otimes \hat{S}$ and $T = T_{s\text{Vec}} \otimes \hat{T}$ with $\hat{S}$ uniquely determined and $\hat{T}$ determined by some sign choices. The projective group generated by $\hat{S}$ and $\hat{T}$ may be infinite for all choices of $\hat{T}$ as the following example illustrates:

**Example 2.1.** Consider the modular category $SU(2)_{6}$. The label set is $I = \{0, 1, 2, 3, 4, 5, 6\}$. The subcategory $PSU(2)_{6}$ is generated by 4 simple objects with even labels: $X_{0} = 1, X_{2}, X_{4}, X_{6}$. We have $\hat{S} = \frac{1}{\sqrt{4 + 2\sqrt{2}}} \begin{pmatrix} 1 & 1 + \sqrt{2} \\ 1 + \sqrt{2} & -1 \end{pmatrix}$ and $\hat{T} = \begin{pmatrix} 1 & 0 \\ 0 & \pm i \end{pmatrix}$. For either choice of $\hat{T}$ the eigenvalues of $\hat{S}\hat{T}$ are not roots of unity: one checks that they satisfy the irreducible polynomial $x^{16} - x^{12} + \frac{1}{4}x^{8} - x^{4} + 1$, which has non-abelian Galois group and is not monic over $\mathbb{Z}$.

### 2.2. The $\theta$-subgroup of $\text{SL}(2, \mathbb{Z})$

The index 3 subgroup $\Gamma_{\theta} < \text{SL}(2, \mathbb{Z})$ generated by $s$ and $t^{2}$ has a uniform description (see e.g. [21]):

$$\Gamma_{\theta} = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) : ac \equiv bd \equiv 0 \pmod{2} \}.$$  

The notation $\Gamma_{\theta}$ comes from the fact that Jacobi’s $\theta$ series $\theta(z) := \sum_{n=-\infty}^{\infty} e^{\pi i z}$ is a modular form of weight $1/2$ on $\Gamma_{\theta}$. Moreover, $\Gamma_{\theta}$ is isomorphic to $\Gamma_{0}(2)$, the Hecke congruence subgroup of level 2 defined as those matrices in $\text{SL}(2, \mathbb{Z})$ that are upper triangular modulo 2, and $\Gamma(2)$ is a subgroup of both $\Gamma_{0}(2)$ and $\Gamma_{\theta}$. In particular $\Gamma_{0}(2)$ and $\Gamma_{\theta}$ are distinct, yet isomorphic, congruence subgroups of level 2. An explicit isomorphism $\vartheta : \Gamma_{\theta} \rightarrow \Gamma_{0}(2)$ is given by $\vartheta(g) = MgM^{-1}$ where $M = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$.

This can be verified directly, via:

$$M \begin{pmatrix} a & b \\ c & d \end{pmatrix} M^{-1} = \begin{pmatrix} a + c & \frac{d + b - a - c}{2} \\ 2c & d - c \end{pmatrix}.$$  

Observe that $\vartheta(\Gamma(n)) = \Gamma(n)$ for any $n$, and for $n$ even $\Gamma(n) \not< \Gamma_{\theta}$. In particular, we see that $\Gamma_{\theta}/\Gamma(n) < \text{SL}(2, \mathbb{Z})/\Gamma(n)$ is isomorphic to an index 3 subgroup of $\text{SL}(2, \mathbb{Z}/n\mathbb{Z})$ that is not normal. Suppose $\varphi : \Gamma_{\theta} \rightarrow H$ has kernel a congruence subgroup, i.e. $\Gamma(n) < \ker(\varphi)$. The congruence level of $\ker(\varphi)$, i.e. the minimal $n$ with $\Gamma(n) < \ker(\varphi)$, is the minimal $n$ so that $\Gamma_{\theta}/\Gamma(n) \rightarrow \varphi(\Gamma_{\theta})$. The following provides a characterization of such quotients:

**Lemma 2.1.** Suppose that $n = 2^{k}q$ with $k \geq 1$ and $q$ odd. Denote by $P_{k}$ a 2-Sylow subgroup of $\text{SL}(2, \mathbb{Z}/2^{k}\mathbb{Z})$. Then,

$$\Gamma_{\theta}/\Gamma(n) \cong P_{k} \times \text{SL}(2, \mathbb{Z}/q\mathbb{Z}).$$  

**Proof.** By the Chinese Remainder Theorem, non-normal index 3 subgroups of

$$\text{SL}(2, \mathbb{Z}/n\mathbb{Z}) \cong \prod_{p|n} \text{SL}(2, \mathbb{Z}/p^{\ell(p)}\mathbb{Z})$$

correspond to non-normal index 3 subgroups of $\text{SL}(2, \mathbb{Z}/2^{k}\mathbb{Z})$ where $n = \prod_{p|n} p^{\ell(p)}$ is the prime factorization of $n$. Any 2-Sylow subgroup of $\text{SL}(2, \mathbb{Z}/2^{k}\mathbb{Z})$ has index 3 and is not normal (since reduction modulo 2 gives a surjection to $\text{SL}(2, \mathbb{Z}/2\mathbb{Z}) \cong \mathfrak{S}_{3}$) so it is enough to show that this fails for $\text{SL}(2, \mathbb{Z}/p^{k}\mathbb{Z})$ with $p > 2$.

In general, if $H < G$ is a non-normal subgroup of index 3 then the (transitive) left action of $G$ on the coset space $G/H$ provides a homomorphism to the symmetric group on 3 letters: $\phi : G \rightarrow \mathfrak{S}_{3}$. If $\phi(G) = \mathfrak{A}_{3}$ (the alternating group on 3 letters) then we would have $\ker(\phi) = H < G$. Thus
\( \phi(G) = \mathfrak{S}_3 \), so that any such group \( G \) must have an irreducible 2 dimensional representation with character values \( 2, -1, 0 \).

By \cite{26} \cite{19} we see that for \( p > 2 \), the groups \( \text{SL}(2, \mathbb{Z}/p^k\mathbb{Z}) \) only have 2-dimensional irreducible representations for \( p = 3, 5 \), and each of these representations factor over the reduction modulo \( p \) map \( \text{SL}(2, \mathbb{Z}/p^k\mathbb{Z}) \to \text{SL}(2, \mathbb{Z}/p\mathbb{Z}) \). By inspection neither \( \text{SL}(2, \mathbb{Z}/3\mathbb{Z}) \) nor \( \text{SL}(2, \mathbb{Z}/5\mathbb{Z}) \) have \( \mathfrak{S}_3 \) as quotients.

\[ \Box \]

3. Main Results

In this section we prove Conjecture \cite{11} for any super-modular category that admits a minimal (spin) modular extension.

3.1. Spin Modular Categories. A spin modular category \( \mathcal{C} \) is a modular category with a (chosen) fermion. Let \( \mathcal{C} \) be a spin modular category, with fermion \( \psi \), (unnormalized) \( S \)-matrix \( \hat{S} \) and \( T \)-matrix \( T \). Proposition II.3 of \cite{12} provides a number of useful symmetries of \( \hat{S} \) and \( T \):

1. \( \hat{S}_{\psi,\alpha} = \epsilon_\alpha d_\alpha \), where \( \epsilon_\alpha = \pm 1 \) and \( \epsilon_\psi = 1 \).
2. \( \theta_{\psi,\alpha} = -\epsilon_\alpha \theta_\alpha \).
3. \( \hat{S}_{\psi,\alpha,\beta} = \epsilon_\beta \hat{S}_{\alpha,\beta} \).

We have a canonical \( \mathbb{Z}/2\mathbb{Z} \)-grading \( \mathcal{C}_0 \oplus \mathcal{C}_1 \) with simple objects \( X \in \mathcal{C}_0 \) if \( \epsilon_X = 1 \) and \( X \in \mathcal{C}_1 \) when \( \epsilon_X = -1 \). The trivial component \( \mathcal{C}_0 \) is a super-modular category, since \( \mathcal{C}_0 = \langle \psi \rangle \cong \text{sVec} \).

Since \( \theta_X = -\epsilon_X \theta_\psi \) it is clear that \( \psi X \not\cong X \) for \( X \in \mathcal{C}_0 \). However, objects in \( \mathcal{C}_1 \) may be fixed by \( - \otimes \psi \) or not. This provides another canonical decomposition \( \mathcal{C}_1 = \mathcal{C}_v \oplus \mathcal{C}_\sigma \) as abelian categories, where a simple object \( X \in \mathcal{C}_v \subset \mathcal{C}_1 \) if \( \psi X \not\cong X \) and \( X \in \mathcal{C}_\sigma \subset \mathcal{C}_1 \) if \( \psi X \cong X \). Finally, using the action of \( - \otimes \psi \) we make a (non-canonical) decomposition of \( \mathcal{C}_0 = \hat{\mathcal{C}}_0 \oplus \psi \hat{\mathcal{C}}_0 \) and \( \mathcal{C}_v = \hat{\mathcal{C}}_v \oplus \psi \hat{\mathcal{C}}_v \) so that when \( X \in \hat{\mathcal{C}}_0 \) we have \( X \psi \in \psi \hat{\mathcal{C}}_0 \) and similarly for \( \mathcal{C}_v \). Notice that for \( X \in \mathcal{C}_0 \) we have \( X^* \not\cong \psi \otimes X \) since \( \theta_X = \theta_{X^*} \), so that we may ensure \( X \) and \( X^* \) are both in \( \mathcal{C}_0 \) or both in \( \psi \mathcal{C}_0 \). On the other hand, for \( Y \in \mathcal{C}_v \) it is possible that \( X^* \cong \psi \otimes X \)–for example, this occurs for \( \text{SO}(2)_1 \).

As in \cite{3} we choose an ordered basis \( \Pi = \Pi_0 \sqcup \Pi_0 \sqcup \Pi_v \sqcup \Pi_v \sqcup \Pi_v \) for the Grothendieck ring of \( \mathcal{C} \) that is compatible with the above partition \( \mathcal{C} = \hat{\mathcal{C}}_0 \oplus \psi \hat{\mathcal{C}}_0 \oplus \hat{\mathcal{C}}_v \oplus \psi \hat{\mathcal{C}}_v \oplus \mathcal{C}_\sigma \). Using \cite{12} Proposition II.3] we have the block matrix decomposition for the \( S \) and \( T \) matrices:

\[
S = \begin{pmatrix}
\frac{1}{2} \hat{S} & \frac{1}{2} \hat{S} & A & A & X \\
\frac{1}{2} \hat{S} & \frac{1}{2} \hat{S} & -A & -A & -X \\
A^T & -A^T & B & -B & 0 \\
B^T & -B^T & B & -B & 0 \\
X^T & -X^T & 0 & 0 & 0
\end{pmatrix}, \quad T = \begin{pmatrix}
\hat{T} & 0 & 0 & 0 & 0 \\
0 & -\hat{T} & 0 & 0 & 0 \\
0 & 0 & \hat{T}_v & 0 & 0 \\
0 & 0 & 0 & \hat{T}_v & 0 \\
0 & 0 & 0 & 0 & T_\sigma
\end{pmatrix}.
\]

Here \( B \) and \( \hat{S} \) are symmetric matrices, and each of \( \hat{T}, \hat{T}_v \) and \( T_\sigma \) are diagonal matrices.

Now consider the following ordered partitioned basis:

1. \( \Pi_0^+ := \{ X_i + \psi X_i : X_i \in \Pi_0 \} \),
2. \( \Pi_0^- := \{ X_i - \psi X_i : X_i \in \Pi_0 \} \),
3. \( \Pi_v^+ := \{ Y_i + \psi Y_i : Y_i \in \Pi_v \} \),
3.2. Case study

level can be lower: for a trivial example we consider the super-modular category sVec. In this case \( \hat{\rho} \) level at most we have a surjection \( \rho \colon C \to N \) that this can only happen if \( \Gamma(N) < \ker(\rho) \). The discussion above now implies \( \Gamma(N) < \ker(\rho) \). Hence, we have shown that \( \ker(\hat{\rho}) \) is a congruence subgroup of level at most \( N \), and in particular \( \hat{\rho} \) has finite image.

Proof. Let \( S \) and \( T \) be the \( S \)-matrix and \( T \)-matrix of \( C \). Consider the projective representation \( \rho \) of \( \text{SL}(2, \mathbb{Z}) \) defined by \( \rho(s) = S \) and \( \rho(t) = T \). By Theorem 1.1, \( \ker(\rho) \) is a congruence subgroup of level \( N \), i.e. \( \Gamma(N) < \ker(\rho) \). Now the restriction of \( \rho \) to \( \Gamma \) has \( \ker(\rho_{|\Gamma}) = \ker(\rho) \cap \Gamma \). However, since \( C \) contains a fermion \( N \) is even, so \( \Gamma(N) < \Gamma(2) \). Hence, \( \Gamma(N) \cap \Gamma = \Gamma(N) \). It follows that \( \Gamma(N) < \ker(\rho_{|\Gamma}) \). The discussion above now implies \( \Gamma(N) < \ker(\rho_{|\Gamma}) < \ker(\hat{\rho}) \) as we have a surjection \( \rho(\Gamma) \to \hat{\rho}(\Gamma) \). Thus, we have shown that \( \ker(\hat{\rho}) \) is a congruence subgroup of level at most \( N \), and in particular \( \hat{\rho} \) has finite image.

3.2. Further Questions. The charge conjugation matrix \( C \) in the basis above has the form \( C'_{i,j} = \pm \delta_{i,j'} \). Since we have arranged that \( X_i \in \Pi_0 \) implies \( X_i^* \in \Pi_0 \), \( C'_{i,j} = -1 \) can only occur for \( i = j \in \Pi_0^- \): if \( (W - \psi W)^* = -(W - \psi W) \) for some simple object \( W \), then \( W^* = \psi W \). We see that this can only happen if \( W \in \mathcal{C}_v \) by comparing twists. Under this change of basis, we have \( \langle S' \rangle^2 = \dim(C)C' \) and \( \langle S'T' \rangle^3 = \frac{1}{24} \langle S' \rangle^2 \). It would be interesting to explore the extra relations among the various submatrices of \( S' \) and \( T' \).

The 16 spin modular categories of dimension 4 are of the form \( SO(n)_1 \) (where \( SO(n)_1 \cong SO(m)_1 \) if and only if \( n \equiv m \mod 16 \)). For \( n \) odd \( SO(n)_1 \) has rank 3 whereas for \( n \) even \( SO(n)_1 \) has rank 4. For example, the Ising modular category corresponds to \( n = 1 \) and \( SO(2)_1 \) has fusion rules like the group \( \mathbb{Z}_4 \). For any modular category \( D \) and \( 1 \leq n \leq 16 \) the spin modular category \( SO(n)_1 \otimes D \) with fermion \( (\psi, 1) \) has either \( C_\sigma = \emptyset \) or \( C_v = \emptyset \). An interesting problem is to classify spin modular categories with either \( C_\sigma = \emptyset \) or \( C_v = \emptyset \), particularly those with no \( \mathbb{Z} \)-factorization.

4. A Case Study

Our result gives an upper bound on the level of \( \ker(\hat{\rho}) \) for super-modular categories \( B \) with minimal modular extensions \( \mathcal{C} \): the level of \( \ker(\hat{\rho}) \) is at most the order of the \( T \)-matrix of \( \mathcal{C} \). The actual level can be lower: for a trivial example we consider the super-modular category sVec. In this case \( \hat{\rho} = \hat{T}^2 = I \) so the level \( \ker(\hat{\rho}) \) is 1, yet the order of the \( T \) matrix for its (16) minimal
modular extensions can be 2, 4, 8 or 16. More generally for any split super-modular category $B = D \otimes sVec \subset D \otimes \text{SO}(m) = C$ (with fermion $(1, \psi)$) the ratio of the levels of the kernels of the $\text{SL}(2, \mathbb{Z})$ (for $C$) and $\Gamma_\theta$ (for $B$, i.e. $D$) representations can be $2^k$ for $0 \leq k \leq 4$.

To gain further insight we consider a family of non-split super-modular categories obtained from the spin modular category (see [12, Lemma III.7]) $\text{SU}(2)_{4m+2}$. This has modular data:

$$S_{i,j} := \frac{\sin \left(\frac{(i+1)(j+1)\pi}{4m+4}\right)}{\sin \left(\frac{\pi}{4m+4}\right)}, \quad T_{j,j} := e^{\frac{\pi(j^2+2j)}{8m+8}}$$

where $0 \leq i, j \leq 4m+2$. Since $T$ has order $16(m+1)$, Theorem [14] implies that the image of the projective representation $\rho : \text{SL}(2, \mathbb{Z}) \to \text{PSU}(4m+3)$ defined via the normalized $S$-matrix $S$ and $T$ factors over $\text{SL}(2, \mathbb{Z}/N\mathbb{Z})$ where $N = 16(m+1)$.

The super-modular subcategory $\text{PSU}(2)_{4m+2}$ has simple objects labeled by even $i, j$. The factorization [14] yields the following:

$$\hat{S}_{i,j} := \frac{\sin \left(\frac{(2i+1)(j+1)\pi}{4m+4}\right)}{\Xi \sin \left(\frac{\pi}{4m+4}\right)}, \quad \hat{T}_{j,j} := e^{\frac{\pi(j^2+j)}{2m+2}}$$

(4.1)

for $0 \leq i, j \leq m$, where $\Xi = \frac{1}{\sin \left(\frac{\pi}{4m+4}\right)}$. In [12] all 16 minimal modular extensions of $\text{PSU}(2)_{4m+2}$ are explicitly constructed and each has $T$-matrix of order $16(m+1)$ so that the kernel of the corresponding projective $\text{SL}(2, \mathbb{Z})$ representation is a congruence subgroup of level $16(m+1)$. Our computations suggests the following conjecture, with cases verified using Magma software [10] indicated in parentheses. A sample of the results of these computations are found in Table 1. The notation $\langle n, k \rangle$ indicates the $k$th group of order $n$ in the GAP [20] library of small groups. In the last column, we sometimes give a slightly different description than is indicated in part (f) below.

We include the groups $\hat{\rho}(\Gamma_\theta)$, $A_m' := [A_m, A_m]$ and $\overline{A}_m := A_m/Z(A_m)$. As $\hat{\rho}$ is not necessarily irreducible, we have $\hat{\rho}(\Gamma_\theta) \to \overline{A}_m$. The congruence level of $\ker(\hat{\rho})$ is computed using Lemma 2.1.

**Conjecture 4.1.** Let $A_m$ be the subgroup of $\text{SU}(k)$ generated by $\hat{S}$ and $\hat{T}^2$ associated with $\text{PSU}(2)_{4m+2}$, the quotient $\overline{A}_m := A_m/Z(A_m)$ and the commutator subgroup $A'_m := [A_m, A_m]$. Then

(a) When $m + 1 = q$ is odd, $\overline{A}_m = \overline{A}_{q-1} \cong \text{PSL}(2, \mathbb{Z}/q\mathbb{Z})$ (verified for $2 \leq m \leq 18$).

(b) When $m + 1 = 2^n$ we have $|\overline{A}_m| = |\overline{A}_{2^n-1}| = 2^{3n+1}$ (verified for $1 \leq n \leq 5$).

(c1) If we write $m + 1 = 2^n q$ where $q$ is odd, then $\overline{A}_m \cong \overline{A}_{2^n-1} \times \overline{A}_{q-1}$ (verified for $1 \leq m \leq 14$).

(c2) If we write $m + 1 = 2^n q$ where $q$ is odd $|\overline{A}_m| = 2^{3n+1} q^3 \prod_{p|q} \frac{p^2-1}{2p^2}$ (primes $p$) (verified for $1 \leq m \leq 21$).

(d) For $5 \leq m + 1 = p$ prime $A'_{p-1} \cong \text{SL}(2, \mathbb{Z}/p\mathbb{Z})$ (verified for $4 \leq m \leq 12$).

(e) If we write $m + 1 = 2^n q$ where $q$ is odd, then $A'_m \cong A'_{2^n-1} \times A'_{q-1}$ (verified for $1 \leq m \leq 14$).

(f) For $m + 1 \not\equiv 0 \mod 4$, we have $A'_m < \hat{\rho}(\Gamma_\theta)$ and $\hat{\rho}(\Gamma_\theta)$ is an iterated semidirect product of $A'_m$ with cyclic group actions (verified for $1 \leq m \leq 14$). In general, $\ker(\hat{\rho})$ is a congruence subgroup of level $4(m+1)$ (verified for $1 \leq m \leq 12$).
Table 1. A Sample of PSU(2)_{4k+2} Results

| m  | |A_m|       | A_m       | \hat{\rho}(\Gamma_\theta) |
|----|-------|----------|-----------|--------------------------|
| 1  | 2^4   | D_{16}   | Z/8Z      | D_{16} = A'_m \times Z/2Z |
| 2  | 12    | PSL(2,Z/3Z) | Q_8        | SL(2,Z/3Z) \times Z/2Z |
| 3  | 2^4   | (128,71) | (64,184)  | (128,71)                  |
| 4  | 60    | PSL(2,Z/5Z) | SL(2,Z/5Z) | A'_4 \times Z/2Z         |
| 5  | 2^4 \cdot 12 | D_{16} \times PSL(2,Z/3Z) | Z/8Z \times Q_8 | (Z/8Z \times SL(2,Z/3Z)) \times Z/2Z |
| 6  | 168   | PSL(2,Z/7Z) | SL(2,Z/7Z) | A'_6 \times Z/2Z         |
| 7  | 2^{10} | A_7      | \cdot | = 2^9                      | A_7                                      |
| 8  | 324   | PSL(2,Z/9Z) | (Z/3Z)^3 \times Q_8 | (A'_8 \times Z/3Z) \times Z/2Z |
| 9  | 2^4 \cdot 60 | D_{16} \times PSL(2,Z/5Z) | Z/8Z \times SL(2,Z/5Z) | A'_9 \times Z/2Z         |
| 10 | 660   | PSL(2,Z/11Z) | SL(2,Z/11Z) | A'_{10} \times Z/2Z      |
| 11 | 2^4 \cdot 12 | (128,71) \times PSL(2,Z/3Z) | (64,184) \times Q_8 | SL(2,Z/3Z) \times (128,71) |
| 12 | 1092  | PSL(2,Z/13Z) | SL(2,Z/13Z) | SL(2,Z/13Z) \times Z/2Z |
| 13 | 2^4 \cdot 168 | D_{16} \times PSL(2,Z/7Z) | Z/8Z \times SL(2,Z/7Z) | A'_{13} \times Z/2Z      |
| 14 | 720   | PSL(2,Z/15Z) | Q_8 \times SL(2,Z/5Z) | SL(2,Z/15Z) \times Z/2Z |

Appendix: Magma Code

For our computational experiments we used the symbolic algebra software Magma [10]. In this appendix we give some basic pseudo-code and some sample Magma code to illustrate how we found the image of \( \hat{\rho}(\Gamma_\theta) \) in our case study, so that the interested reader can do similar explorations. Given an integer \( m \), the \((m + 1) \times (m + 1)\) \( \hat{S} \) and \( \hat{T}^2 \) matrices obtained from PSU(2)_{4m+2} are given in equation (4.1). In order to use the Magma software we express the entries of \( \hat{S} \) and \( \hat{T}^2 \) in the cyclotomic field \( \mathbb{Q}(\omega) \), where \( \omega \) is an \((8m + 8)\)-th root of unity. For this we must write \( \sin \left( \frac{(2i+1)(2j+1)\pi}{4m+4} \right) \) and \( \sqrt{2(m+1)} \) in terms of \( \omega \) for which we use the result of generalized form of quadratic Gauss sums [1].

Here is the pseudocode to find \( \hat{\rho}(\Gamma_\theta) \) for PSU(2)_{4m+2}:

algorithm \text{projective image}

input: integer \( m \)
output: \( \hat{\rho}(\Gamma_\theta) \)

set \( K \) to be the cyclotomic field \( \mathbb{Q}(\omega) \), where \( \omega \) is an \((8m + 8)\)-th root of unity.
set \( M = 2(m + 1) \)
initialize \( S \) and \( T^2 \) to be \((m + 1) \times (m + 1)\) zero matrices over \( K \).
initialize \( \alpha = 0 \).

step 1: calculate \( \alpha \)
if \( M \equiv 0 \pmod{4} \) return \( \alpha = \sum_{n=0}^{M-1} \omega^{4n^2} / (1 + \omega^M) \)
else consider \( M/2 = m + 1 \pmod{4} \). Notice there are only two cases: \( m + 1 \equiv 1 \pmod{4} \) and \( m + 1 \equiv 3 \pmod{4} \).
if \( m + 1 \equiv 1 \pmod{4} \) return \( \alpha = \frac{\omega^{m+1} - \omega^{-m+1}}{\omega^{2m+2}} \sum_{n=0}^{m} \omega^{8n^2} / (\omega^M) \)
else return \( \alpha = \frac{\omega^{m+1} - \omega^{-m+1}}{\omega^{2m+2}} \sum_{n=0}^{m} \omega^{8n^2} / (\omega^M) \)
return $\alpha = 2/\alpha$.

step 2: define the entries
\[
\text{for } 1 \leq i,j \leq m+1, S_{i,j} = \alpha \frac{\omega^{(2i-1)(2j-1)} - \omega^{-(2i-1)(2j-1)}}{2(\omega^M)} \text{ and } T_{2j,j} = \omega^{(2(j-1))^2 + 4(j-1)}
\]

step 3: find the projective image
set $A$ to be the matrix group generated by $S$ and $T_2$ defined above, and $ZK$ the group of scalar matrices over $K$. The projective image of $A$ is then $A/(ZK \cap A)$.

The following code can be used in Magma \[10\] to find the $\hat{\rho}(\Gamma_\theta)$ in this case, and slight modifications will give the other headings of Table \[1\]

```magma
m:=1;
K<w>:= CyclotomicField(8*m+8);
GL:=GeneralLinearGroup(m+1,K);
M:=2*(m+1);
alpha:=0;
if M mod 4 eq 0 then
  for n:=0 to M-1 do
    alpha:=alpha + w^(4*(n^2));
  end for;
  alpha:=alpha/(w^M+1);
else
  if (m+1) mod 4 eq 1 then
    for n:=0 to m do
      alpha:= alpha + w^(8*n^2);
    end for;
    alpha:=alpha/(w^M);
  else
    for n:=0 to m do
      alpha:=alpha + w^(8*(n^2));
    end for;
    alpha:=alpha/(w^M);
  end if;
  alpha:=(w^(m+1) - w^(-(m+1)))/(w^(2*m+2))*alpha;
end if;
alpha:=2/alpha;
S:=ZeroMatrix(K,m+1,m+1);
for i:=1 to m+1 do
  for j:=1 to m+1 do
    S[i,j]:=(w^((2*i-1)*(2*j-1))-w^(-(2*i-1)*(2*j-1)))/(2*(w^M));
    S[i,j]:=S[i,j]*alpha;
  end for;
end for;
T2:=ZeroMatrix(K,m+1,m+1);
for j:=1 to m+1 do
  T2[j,j]:=w^((2*(j-1))^2 + 4*(j-1));
end for;
```

9
A:=MatrixGroup<m+1,K|S,T2>;
ZK:=MatrixGroup<m+1,K|w*IdentityMatrix(K,m+1)>
F:=(A/(A meet ZK));
Microsoft Research Station Q, University of California, Santa Barbara, CA U.S.A.

E-mail address: rowell@math.tamu.edu

Department of Mathematics, Texas A&M University, College Station, TX U.S.A.

E-mail address: zhenghwa@microsoft.com

Microsoft Research Station Q and Department of Mathematics, University of California, Santa Barbara, CA U.S.A.

E-mail address: zhangqing@math.tamu.edu

Department of Mathematics, Texas A&M University, College Station, TX U.S.A.