Journal of Number Theory 224 (2021) 274–306

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Elliptic curves and Thompson's sporadic simple group

Maryam Khaqan

Department of Mathematics, Emory University, 400 Dowman Drive, Atlanta, GA 30322, United States of America

ARTICLE INFO

Article history:
Received 17 August 2020
Received in revised form 15 January 2021
Accepted 29 January 2021
Available online 23 February 2021
Communicated by L. Smajlovic

MSC:
11F22
11F37

Keywords:
Moonshine
Number theory
Sporadic groups
Finite groups
Discrete groups
Modular forms
Harmonic Maaß forms
Birch and Swinnerton-Dyer Conjecture
L-function
Elliptic curves
Selmer group
Mock modular forms
Rademacher sums
Quadratic forms
Traces of singular moduli

ABSTRACT

We characterize all infinite-dimensional graded virtual modules for Thompson's sporadic simple group whose graded traces are weight $\frac{3}{2}$ weakly holomorphic modular forms satisfying certain special properties. We then use these modules to detect the non-triviality of Mordell–Weil, Selmer, and Tate-Shafarevich groups of quadratic twists of certain elliptic curves.

E-mail address: maryam.khaqan@emory.edu.

https://doi.org/10.1016/j.jnt.2021.01.015
0022-314X/

1. Introduction

In 1978, McKay and Thompson observed [59] that the first few coefficients of the normalized elliptic modular invariant $J(\tau) = q^{-1} + 196884q + 21493760q^2 + 864299970q^3 + O(q^4)$, a central object in the theory of modular forms, can be written as sums involving the first few dimensions of irreducible representations of the monster group $\mathbb{M}$, e.g.,

$$\begin{aligned} 196884 &= 1 + 196883 \\ 21493760 &= 1 + 196883 + 21296876 \\ 864299970 &= 2 \cdot 1 + 2 \cdot 196883 + 21296876 + 842609326. \end{aligned} \tag{1.1}$$

This coincidence inspired Thompson's conjecture [58] that there is an infinite-dimensional $\mathbb{M}$-module $V = \bigoplus_{n \geq -1} V_n$ whose graded dimension is $J(\tau)$ and whose McKay–Thompson series

$$T_g(\tau) := \sum_{n \geq -1} \operatorname{tr}(g|V_n) q^n \tag{1.2}$$

are distinguished functions on the upper half-plane. Conway and Norton [16] explicitly described the relevant McKay-Thompson series, and also christened this phenomenon "monstrous moonshine." Their conjecture was proven by Borcherds [4] (building on work by Frenkel, Lepowsky and Meurman [28]) in 1992. In the few decades since the first observations of McKay and Thompson, it has become clear that monstrous moonshine is just the first of a series of similar phenomena encompassing several finite groups and their counterparts in the world of modular forms.

Generalized moonshine [9] (see also [41,16,45]), for example, relates various subquotients of the Monster to other weight zero modular forms. Umbral moonshine [12,13] (see also [22,29] and [14]), on the other hand, relates the 23 umbral groups (each of which is a quotient of the automorphism group of one of the 23 Niemeier lattices) to weight $\frac{1}{2}$ *mock modular forms*. Thompson moonshine, conjectured by Harvey and Rayhaun [33] in 2015 and proven by Griffin and Mertens in [31], involves Thompson's sporadic simple group Th, and certain weight $\frac{1}{2}$ modular forms. (We remark here that the Thompson group, being a subgroup of the Monster, also appears in the generalized moonshine setting mentioned above. For the purpose of this paper, "Thompson moonshine" refers to the Harvey and Rayhaun version.)

Recently, in [23,24], Duncan, Mertens, and Ono discovered the first instance of moonshine for the O'Nan group, one of the so-called pariah groups (i.e., a sporadic simple group which is not a subquotient of the monster group), where the functions involved are modular forms of weight $\frac{3}{2}$. Their work is not only a contribution to the theory of moonshine, it also serves another important purpose: In the same paper, they use their O'Nan-module to study properties of quadratic twists of certain elliptic curves and thus

use moonshine to provide insight into objects that are central to current research in number theory.

While number theory's contribution to moonshine is ubiquitous and irrefutable, O'Nan moonshine is one of the first instances where we see moonshine's direct contribution to number theory. Such a role-reversal is our primary motivation for this work.

We begin this work by proving the existence of a family of infinite-dimensional graded Th-modules whose McKay–Thompson series are weight $\frac{3}{2}$ modular forms that satisfy certain properties (see Theorem 3.2). The techniques we use to prove this are similar to ones used in Griffin and Mertens' work [31] to prove the Thompson moonshine conjecture [33]. (These techniques were first suggested by Thompson, and subsequently used by Atkin, Fong and Smith [26,53] to prove monstrous moonshine abstractly.) On the other hand, our McKay–Thompson series are weight $\frac{3}{2}$ modular forms (in contrast to the weight $\frac{1}{2}$ forms of [33]) and the role played by theta functions in their paper is taken up by weight $\frac{3}{2}$ cusp forms in ours. The involvement of weight $\frac{3}{2}$ cusp forms allows us to employ an approach similar to Duncan, Mertens, and Ono (in [23,24]): We exploit the existing relationship between these forms and elliptic curves to study geometric invariants of various elliptic curves. This is the content of Theorems 1.1 and 1.3.

Our result regarding the existence of a family of Thompson modules is, in fact, a classification result. We classify all infinite-dimensional graded modules $W = \bigoplus W_n$ (see Theorem 3.2) for the Thompson group whose McKay–Thompson series take the form

$$\mathcal{F}_g(\tau) := 6q^{-5} + \sum_{n>0} \operatorname{tr}(g|W_n)q^n \tag{1.3}$$

and satisfy the following properties (cf. Proposition 3.1):

(1) For each $g \in Th$, the corresponding McKay–Thompson series $\mathcal{F}_g(\tau)$ is a weight $\frac{3}{2}$ weakly holomorphic modular form of a specific level and multiplier system, and satisfies the Kohnen plus space condition.
(2) Each McKay–Thompson series $\mathcal{F}_g(\tau)$ has integer coefficients and is uniquely determined — up to the addition of certain cusp forms — by its polar parts at the cusps, which are specified in a uniform way. (See Section 3 for details.)

We note here that properties (1) and (2) listed above ensure that the functions $\mathcal{F}_g(\tau)$ are, up to the addition of cusp forms, simply Rademacher sums projected to the Kohnen plus space (see Section 2 for background on Rademacher sums).

The connection between Rademacher sums and moonshine was first proposed in [21], where the McKay–Thompson series that appear in monstrous moonshine were characterized completely in terms of Rademacher sums of weight 0. In particular, it was shown that the so-called *genus-zero property* of monstrous moonshine is equivalent to the fact that the McKay–Thompson series of the Monster module coincide (up to a constant) with corresponding Rademacher sums of weight 0. It was later argued in [11,12] that

the correct analogue of the genus zero property in the case of Umbral (and Mathieu) moonshine is that the corresponding McKay–Thompson series must coincide with the relevant Rademacher sums in each case (see also [14,20]). Here we take this perspective and hence consider it natural, from the point of view of moonshine, to ask for our McKay–Thompson series to satisfy the properties listed above.

To prove our classification result, we first construct spaces of weakly holomorphic modular forms of the appropriate level and multiplier for each $g \in Th$. We use Rademacher sums and eta-quotients to do this. Since we can explicitly compute the Fourier coefficients of these forms at various cusps, we can restrict our attention to the subspace of forms that satisfy properties (1) and (2). For a collection of these forms to be the McKay–Thompson series of a virtual module (as in Theorem 3.2), they must satisfy congruences modulo certain powers of primes that divide the order of the Thompson group (see Section 4). A complete description of these congruences can be obtained using Thompson's reformulation ([53]) of Brauer's characterization of generalized characters. We prove that our alleged McKay–Thompson series satisfy the congruences mentioned above in Section 4. We note here that it would be interesting to consider the analogous classification for the O'Nan group, building on the work already done in [24].

Once we have proven the existence of the Thompson modules, we use their properties to help detect the non-triviality of Mordell–Weil, Selmer, and Tate–Shafarevich groups of quadratic twists of certain elliptic curves (see Theorems 1.1 and 1.3). To state our main results, we let E be an elliptic curve over $\mathbb{Q}$, and for $d < 0$ a fundamental discriminant, we let E^d denote the d^{th} quadratic twist of E. (We refer the reader to [40,50] and [55] for background on elliptic curves.) We further let $E(\mathbb{Q})$ denote the set of $\mathbb{Q}$-rational points on E, i.e., the set of points on E whose coordinates are rational numbers. Then, $E(\mathbb{Q})$ has the structure of a finitely generated abelian group (by the Mordell–Weil theorem [50]), i.e., $E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}$. Here $r \in \mathbb{Z}_{\geq} 0$ is called the (algebraic) rank of E, and $E(\mathbb{Q})_{\text{tor}}$ is a finite abelian group. Computing the rank of a general elliptic curve is considered a hard problem in number theory.

One way of approaching this problem is to study the L-function associated to E, defined for $s \in \mathbb{C}$ with $\text{Re}(s) > \frac{3}{2}$ by

$$L_E(s) = \prod_{p \text{ prime}} \left(1 - a_p p^{-s} + \epsilon(p) p^{1-2s}\right)^{-1}. \tag{1.4}$$

Here, $a_p := p + 1 - \#E(\mathbb{F}_p)$ where $E(\mathbb{F}_p)$ is the group of $\mathbb{F}_p$-rational points on the mod p reduction of E, and $\epsilon(p) \in \{0, 1\}$ (see [50] for a precise definition and further discussion on L-functions). The (weak) *Birch and Swinnerton-Dyer Conjecture* states that the order of vanishing of $L_E(s)$ at $s = 1$ is equal to the rank r of E. Thus, studying the behavior of $L_E(s)$ near $s = 1$ is one way of tackling the problem of computing the rank of E.

Note that *a priori*, the product in eq. (1.4) only converges for $\text{Re}(s) > \frac{3}{2}$, so part of the conjecture is that $L_E(s)$ can be analytically continued to a function that converges near $s = 1$. This part follows from the Modularity Theorem (proven in [6] by extending

the results of [62,56]), which states that corresponding to every elliptic curve over $\mathbb{Q}$, there exists a weight 2 newform of level equal to the conductor of E, whose L-function coincides with $L_E(s)$. The L-function associated to a cusp form $f = \sum_{n=1}^{\infty} a_n q^n$ of weight k is defined on $\mathrm{Re}(s) > 1 + \frac{k}{2}$ and extends analytically to a holomorphic function on $\mathbb{C}$ [2]. Hence it is possible to talk about the behavior of $L_E(s)$ as $s \to 1$, for example. The Birch and Swinnerton-Dyer Conjecture has been proven in special cases (see for example [3]). In particular, it is known that if $L_E(1) \neq 0$, then $E(\mathbb{Q})$ is finite [32,38]. We will use this result to prove our first theorem about elliptic curves.

To state our results, we let

$$\mathcal{F}(\tau) = 6(q^{-5} + 85995q^3 - 565760q^4 + 52756480q^7 - 190356480q^8 + O(q^{11})) \tag{1.5}$$

be the unique weakly holomorphic modular form of weight $\frac{3}{2}$ and level 4 in the plus space whose Fourier expansion is of the form $\mathcal{F}(\tau) = 6q^{-5} + O(q)$. (Note that $\mathcal{F}(\tau)$ is relevant for us because for each of the graded Th-modules $W = \bigoplus_{n>0} W_n$ described in Theorem 3.2, the graded dimension of W is $\mathcal{F}(\tau)$.) Let $c(d)$ denote the $|d|^{th}$ Fourier coefficient in the expansion of $\mathcal{F}(\tau)$. We denote by $\left(\frac{m}{n}\right)$ the usual Kronecker symbol [15], then we have the following theorem.

Theorem 1.1. *Let $d < 0$ be a fundamental discriminant which satisfies $\left(\frac{d}{19}\right) = -1$. Let E be an elliptic curve of conductor 19, and let E^d denote the d^{th} quadratic twist of E. If $c(d) \not\equiv 0 \pmod{19}$, then the Mordell–Weil group $E^d(\mathbb{Q})$ is finite.*

We can state a stronger result for elliptic curves of conductor 14, one which depends on a local version of the strong form of Birch and Swinnerton-Dyer Conjecture. To do this, we first establish some notation.

For E an elliptic curve of rank r, let $\#E(\mathbb{Q})_{\mathrm{tor}}$ denote the order of the torsion subgroup of the $\mathbb{Q}$-rational points of E and let $\#Ш(E)$ be the order of the Tate–Shafarevich group of E. Then the strong form of the Birch and Swinnerton-Dyer Conjecture states the following [63].

Conjecture 1.2 *(The Birch and Swinnerton-Dyer Conjecture). The rank r of an elliptic curve E over Q equals the order of vanishing of $L_E(s)$ at $s = 1$. Moreover, we have*

$$\frac{L_E^{(r)}(1)}{r!\Omega(E)} = \#Ш(E)\ \frac{\mathrm{Reg}(E)\prod_l c_l(E)}{\left(\#E(\mathbb{Q})_{\mathrm{tor}}\right)^2}, \tag{1.6}$$

where $L_E^{(r)}(s)$ is the r^{th} derivative of $L_E(s)$.

The left-hand side of Equation (1.6) ties together the rank of the elliptic curve and the value of the r^{th} derivative of the L-function at $s = 1$. It has been proven to always be a rational number [1]. On the right-hand side, all quantities except $\#Ш(E)$ are effectively

computable invariants of an elliptic curve (see Section 5 for details). The Tate-Shafarevich group $Ш(E)$, however, is not even known to be finite except for special cases.

So we instead turn to a relatively simple object. Given p a prime, we define $Ш(E)[p]$ to be the set consisting of elements of the Tate–Shafarevich group with order dividing p. Then, $Ш(E)[p]$ is finite for all p. This follows from the finiteness of a related object: the p-Selmer group $\mathrm{Sel}_p(E)$ of E, which fits into a short exact sequence

$$1 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E) \to Ш(E)[p] \to 1. \tag{1.7}$$

The Selmer group of an elliptic curve over $\mathbb{Q}$ is known to be finite for every p (see [50]), so we have that $Ш(E)[p]$ is finite for every p. Also by the short exact sequence, we get that if $\mathrm{Sel}_p(E)$ is trivial for any prime p then $E(\mathbb{Q})$ is finite, i.e., E has rank 0.

In this work, we will use the family of Thompson modules whose existence is proven in Theorem 3.2 to develop a criterion to check whether the p-Selmer groups of quadratic twists of elliptic curves of conductor 14 are trivial. More precisely, we let E be an elliptic curve over $\mathbb{Q}$, and for each $d < 0$ a fundamental discriminant, let E^d denote the d^{th} quadratic twist of E. As we shall prove in Theorem 3.2, there exists an infinite-dimensional graded Th-module $W = \bigoplus_{n>0} W_n$ whose McKay–Thompson series $\mathcal{F}_g(\tau)$ satisfy properties (1) and (2) as above. Then we have the following theorem.

Theorem 1.3. *Let $d < 0$ be a fundamental discriminant for which $\left(\frac{d}{7}\right) = -1$ and $\left(\frac{d}{2}\right) = 1$. Let E be an elliptic curve of conductor 14, and let g denote an element of order 14 in Th. If $\mathrm{tr}(g|W_{|d|}) \not\equiv 0 \pmod{49}$, then the Mordell–Weil group $E^d(\mathbb{Q})$ is finite and $Ш(E^d)[7]$ is trivial. If, on the other hand, $\mathrm{tr}(g|W_{|d|}) \equiv 0 \pmod{49}$ and $\mathrm{tr}(g|W_4) \not\equiv 43 \pmod{56}$, then $\mathrm{Sel}_7(E^d)$ is non-trivial, and if $L_{E^d}(1)$ is non-zero then so is $Ш(E^d)[7]$.*

This is akin to Theorem 1.4 of [24], and our proof will follow along similar lines. One notable difference is that there is no dependence on (generalized) class numbers in the corresponding congruences in our case. We can also write down an analogous statement for elliptic curves of conductor 19, but the techniques we use to prove Theorem 1.3 do not apply in this case (cf. Theorem 5.4), so it is conditional upon the (strong form of the) Birch and Swinnerton-Dyer Conjecture.

We now describe a sketch of the proof of Theorems 1.1 and 1.3. Let $p \in \{7, 19\}$ be the relevant prime in either statement and fix $W = \bigoplus_{n>0} W_n$ to be a virtual Thompson module whose McKay–Thompson series $\mathcal{F}_g(\tau)$ satisfies the properties listed in Theorem 3.2. We then write each $\mathcal{F}_g(\tau)$ for $[g] \in \{14A, 19A\}$ as a sum of traces of singular moduli (cf. Section 5.1) and weight $\frac{3}{2}$ cusp forms. This expression combined with the condition on d in the statement of Theorem 1.1 gives us that the congruence in the statement holds if and only if the relevant cusp form coefficient is divisible by $p = 19$. Thus, if the congruence in the statement of Theorem 1.1 does not hold, then the cusp form coefficient is not divisible by 19, and we can employ a corollary (cf. Lemma 5.3) of Kohnen's work [37] to show that this means $L_{E^d}(1) \neq 0$. Finally, Kolyvagin's work

shows that $E^d(\mathbb{Q})$ is finite. This completes the proof of Theorem 1.1. For Theorem 1.3, we first consider the case that $\operatorname{tr}(g_{14}|W_{|d|}) \not\equiv 0 \pmod{49}$. The expression for $\mathcal{F}_g(\tau)$ in terms of traces of singular moduli and cusp forms implies that the relevant cusp form coefficient is not divisible by $p = 7$. We can utilize Kohnen's work again to conclude that $\operatorname{ord}_p(\frac{L_{E^d}(1)}{\Omega(E^d)}) > 0$. At this point, we use work of Skinner and Urban (Theorem 5.4) which connects $\operatorname{ord}_p(\frac{L_{E^d}(1)}{\Omega(E^d)})$ to the non-triviality of the p-Selmer and Tate-Shafarevich groups of E^d to prove the theorem. A similar argument applies if we assume that $\operatorname{tr}(g_{14}|W_{|d|}) \equiv 0 \pmod{49}$ and $\operatorname{tr}(g_{14}|W_{|4|}) \not\equiv 43 \pmod{49}$.

The rest of this paper is organized as follows. In Section 2 we set up notation and define the terms that appear in Proposition 3.1 and Theorem 3.2. In Section 3 we uniquely characterize the modular forms $\mathcal{F}_g(\tau)$ that satisfy properties (1) and (2) above and prove Proposition 3.1. In Section 4 we prove Theorem 3.2. Finally, in Section 5 we prove Theorems 1.1 and 1.3.

Acknowledgments

The author would like to thank John Duncan for helping initiate this project and his invaluable guidance and support throughout the process. The author thanks Richard Borcherds, John Duncan, Jeff Harvey, Michael Mertens, Brandon Rayhaun, Robert Schneider, and the anonymous referee for helpful comments on an earlier draft.

2. Background and notation

Throughout this paper, we use the notation $e(x) = e^{2\pi i x}$ and $q = e(\tau)$ with τ in the upper half-plane, which we denote $\mathbb{H}$. We also use $\left(\frac{m}{n}\right)$ to denote the Kronecker symbol [15, Algorithm 1.4.10]. We will use the ATLAS [17] notation for conjugacy classes of Th, and understand nAB to mean $nA \cup nB$.

2.1. Rational characters

We define the *rational conjugacy class* of an element $g \in Th$, denoted by $[g]$, to be the set of all elements that are conjugate to an n^{th} power of g where n is relatively prime to the order of g. (In particular, this contains the conjugacy class of g as a subset.)

We recall that a *rational character* of a group G is a character afforded by a $\mathbb{Q}G$-module. By [18, Lemma 39.4], if g and h are in the same rational conjugacy class, and $\phi : G \to \mathbb{Q}$ is a rational character, then $\phi(g) = \phi(h)$. We note that if ϕ is a rational character of Th, then $\phi(g)$ is an algebraic integer lying in $\mathbb{Q}$, so in fact $\phi(g) \in \mathbb{Z}$.

In this paper, we will consider the irreducible rational characters of Th. To describe these, we first define a few things. Let G be a finite group and V be a $\mathbb{C}G$-module. For each field automorphism $\gamma : \mathbb{C} \to \mathbb{C}$, there exists a unique (up to isomorphism) representation V^γ with character $\chi_{V^\gamma(g)} = \gamma\chi_V(g)$. We call V^γ a Galois-conjugate of V. Then, we have the following proposition.

Proposition 2.1. *(See [18, Theorem 74.5], for example.) Let $V_1(=V), V_2 \dots, V_n$ be the distinct Galois-conjugates of an irreducible $\mathbb{C}G$-module V. Then there exists a natural number m_V such that $m_V(V_1 \oplus \cdots \oplus V_n)$ is the complexification of an irreducible $\mathbb{Q}G$-module. Furthermore, each irreducible $\mathbb{Q}G$-module W arises in this way from a unique Galois-class of irreducible $\mathbb{C}G$-modules, i.e.*

$$W \otimes_{\mathbb{Q}} \mathbb{C} \simeq m_V(V_1 \oplus \cdots \oplus V_n). \tag{2.1}$$

The number m_V is called the (rational) Schur index of V. By [25, Section 7], the Schur index is 1 for each irreducible representation of Th. Thus, we can read off the 39 irreducible rational characters of Th directly from the character table. We denote these by $\chi_1, \chi_2, \dots, \chi_{39}$.

2.2. Mock modular forms

To prove the existence of the Thompson modules in Theorem 3.2, we first have to construct weakly holomorphic modular forms of weight $\frac{3}{2}$ with the appropriate level and multiplier. Recall that a *weakly holomorphic modular form* is a function on the upper half-plane that transforms like a modular form, is holomorphic on the upper half-plane and meromorphic at the cusps. One way of constructing spaces of weakly holomorphic forms is to use Rademacher sums, which are *a priori* mock modular forms, and then restrict to the subspace of forms with vanishing shadow. Here we recall the definitions and basic facts that we will need from the theory of mock modular forms and Rademacher sums to describe these functions. We refer the reader to [7,19,43] for more on mock modular forms.

Let $k \in \frac{1}{2}\mathbb{Z}$ and Γ be a subgroup of $\mathrm{SL}_2(\mathbb{R})$ containing $\pm I$ such that Γ is commensurable with $\mathrm{SL}_2(\mathbb{Z})$. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, write $\gamma\tau$ for $\frac{a\tau+b}{c\tau+d}$, and define $\mathrm{j}(\gamma,\tau) = (c\tau+d)^{-2}$. We call a function $\psi : \Gamma \to \mathbb{C}$ a *multiplier system* for Γ of weight k if

$$\psi(\gamma_1\gamma_2)\mathrm{j}(\gamma_1\gamma_2,\tau)^{\frac{k}{2}} = \psi(\gamma_1)\mathrm{j}(\gamma_1,\gamma_2\tau)^{\frac{k}{2}}\psi(\gamma_2)\mathrm{j}(\gamma_2,\tau)^{\frac{k}{2}} \tag{2.2}$$

for each $\gamma_1, \gamma_2 \in \Gamma$, where we choose the principal branch of the logarithm to define the exponential $x \mapsto x^s$ in case s is not an integer.

In this paper we will consider multiplier systems of the form

$$\psi_{4N,v,h}(\gamma) := e\left(-\frac{vcd}{4Nh}\right), \tag{2.3}$$

where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(4N)$ and v, h are integers with $h | \gcd(N, 24)$.

Recall that $\Gamma_0(N)$ is the congruence subgroup

$$\Gamma_0(N) := \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\} \tag{2.4}$$

of the full modular group $\mathrm{SL}_2(\mathbb{Z})$. We can now define the (k,ψ)-action of $\gamma \in \Gamma_0(N)$ on a smooth function $f : \mathbb{H} \to \mathbb{C}$ by

$$(f|_{k,\psi}\gamma)(\tau) := \begin{cases} \psi(\gamma)\mathrm{j}(\gamma,\tau)^{\frac{k}{2}} f(\gamma\tau) & \text{if } k \in \mathbb{Z} \\ \left(\frac{c}{d}\right) \varepsilon_d^{2k} \psi(\gamma)\mathrm{j}(\gamma,\tau)^{\frac{k}{2}} f(\gamma\tau) & \text{if } k \in \frac{1}{2}+\mathbb{Z}, \end{cases} \tag{2.5}$$

where

$$\varepsilon_d := \begin{cases} 1 & d \equiv 1 \pmod 4, \\ i & d \equiv 3 \pmod 4. \end{cases} \tag{2.6}$$

And we assume $4|N$ if $k \notin \mathbb{Z}$.

Definition 2.2. A *harmonic (weak) Maaß form* of *weight* $k \in \frac{1}{2}\mathbb{Z}$, *level* N and *multiplier system* ψ, is a smooth function $f : \mathbb{H} \to \mathbb{C}$ on the upper half-plane that satisfies the following properties:

(1) It is invariant under the (k,ψ)-action by all $\gamma \in \Gamma_0(N)$ and $\tau = u + iv \in \mathbb{H}$.
(2) It is annihilated by the *weight k hyperbolic Laplacian*,

$$\Delta_k f := \left[-v^2\left(\frac{\partial^2}{\partial u^2} + \frac{\partial^2}{\partial v^2}\right) + ikv\left(\frac{\partial}{\partial u} + i\frac{\partial}{\partial v}\right)\right] f \equiv 0. \tag{2.7}$$

(3) There is a polynomial $P_f(q^{-1})$ such that $f(\tau) - P_f(e^{-2\pi i\tau}) = O(e^{-cv})$ for some $c > 0$ as $v \to \infty$. Analogous growth conditions are required at all cusps of $\Gamma_0(N)$.

We denote the space of harmonic Maaß forms of weight k, level N, and multiplier ψ by $H_k(\Gamma_0(N),\psi)$, and we omit the multiplier if it is trivial.

Bruinier and Funke first introduced harmonic Maaß forms in [8]. We are going to need the following two results from their paper.

Lemma 2.3. *[8, equations (3.2a) and (3.2b)] Let $f \in H_k(\Gamma_0(N),\psi)$ be a harmonic Maaß form of weight $k \neq 1$ such that $\psi(\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)) = 1$. Then there is a canonical splitting*

$$f(\tau) = f^+(\tau) + f^-(\tau), \tag{2.8}$$

where for some $m_0 \in \mathbb{Z}$ we have the holomorphic part,

$$f^+(\tau) := \sum_{n=m_0}^{\infty} c_f^+(n) q^n, \tag{2.9}$$

and the non-holomorphic part,

$$f^-(\tau) := \sum_{n=1}^{\infty} \overline{c_f^-(n)} n^{k-1} \Gamma(1-k; 4\pi n v) q^{-n}. \tag{2.10}$$

Here $\Gamma(\alpha; x)$ *denotes the upper incomplete Gamma function.*

We call the holomorphic part of a harmonic Maaß form a *mock modular form*. Let $M_k^!(\Gamma_0(N), \psi)$ denote the space of weakly holomorphic modular forms of weight k, level N, and multiplier system ψ. Then we have the following proposition.

Proposition 2.4. *(See [8, Proposition 3.2].) The operator*

$$\xi_k : H_k(\Gamma_0(N), \psi) \to M_{2-k}\left((\Gamma_0(N), \overline{\psi}\right),\ f \mapsto \xi_k f := 2iv^k \overline{\frac{\partial f}{\partial \overline{\tau}}} \tag{2.11}$$

is well-defined and surjective with kernel $M_k^!(\Gamma_0(N), \psi)$*. Moreover, we have that*

$$(\xi_k f)(\tau) = -(4\pi)^{1-k} \sum_{n=1}^{\infty} c_f^-(n) q^n \tag{2.12}$$

and we call $\xi_k f$ *the* shadow *of (the holomorphic part of)* f*.*

Thus, in particular, a mock modular form is a weakly holomorphic modular form if it has a vanishing shadow. We will construct the desired space of weakly holomorphic forms by first constructing mock modular forms of the appropriate level and weight and then showing that they have vanishing shadows.

2.3. Rademacher sums

To construct the relevant mock modular forms for the proof of Theorem 3.2, we need to recall some facts about Rademacher sums and Rademacher series. See [10,11,21] for more details.

Let $\Gamma_\infty := \left\{ \pm \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z} \right\}$ denote the stabilizer of ∞ in $\Gamma_0(N)$. Then one can define the Rademacher sum of weight $k \geq 1$, level N, multiplier system ψ and index μ, by

$$R_{k,N,\psi}^{[\mu]}(\tau) := \lim_{K \to \infty} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_{K,K^2}(N)} q^\mu |_{k,\psi} \gamma \tag{2.13}$$

where

$$\Gamma_{K,K^2}(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N) : |c| < K \text{ and } |d| < K^2 \right\} \tag{2.14}$$

and $\mu \in \mathbb{Z} + \frac{-i}{2\pi} \log\left(\psi\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\right)$.

When convergent, Rademacher sums define mock modular forms of level N, weight k, and multiplier system ψ. We will use the following important facts from the theory of Rademacher sums, which we condense in one lemma. We will use the following important facts from the theory of Rademacher sums, which we condense in one lemma.

Lemma 2.5. *(See [24, Theorem 2.5], for example.) Let $\mu \leq 0$. Assuming locally uniform convergence, the Rademacher sum $R^{[\mu]}_{k,4N,\psi}(\tau)$ for $k \geq 1$ defines a mock modular form of weight $k \in \mathbb{Z} + \frac{1}{2}$, for $\Gamma_0(4N)$ and multiplier ψ whose shadow is given by a constant multiple of the Rademacher sum $R^{[-\mu]}_{2-k,4N,\overline{\psi}}(\tau)$. The completion of $R^{[\mu]}_{k,4N,\psi}(\tau)$ to a harmonic Maaß form has a pole of order μ at the cusp ∞ and vanishes at all other cusps.*

In this paper, we will be looking at Rademacher sums of weight $\frac{3}{2}$ for $\Gamma_0(4N)$ with multiplier $\psi_{4N,v,h}$ and index $\mu < 0$. In this particular case, it has been proven in [10] that the sums converge locally uniformly and define holomorphic functions on $\mathbb{H}$.

2.4. Kohnen plus space condition

One of the properties that we want our candidate McKay–Thompson series to satisfy is to lie in Kohnen's plus space. Let $S_k(\Gamma_0(N))$ denote the space of weight k cusp forms for $\Gamma_0(N)$. Kohnen's plus space was first introduced by Kohnen (see [35–37]) as the subspace of $S_{k+\frac{1}{2}}(\Gamma_0(4N))$ which consists of all forms whose Fourier coefficients are supported on exponents n with $n \equiv 0, (-1)^k \pmod 4$. We extend this idea to all modular forms and harmonic Maaß forms as follows: We say that a function f in $H_{k+\frac{1}{2}}(\Gamma_0(4N))$ (resp. in $M^!_{k+\frac{1}{2}}(\Gamma_0(4N))$) *satisfies the Kohnen plus space condition* if the Fourier coefficients of f are supported on exponents n with $n \equiv 0, (-1)^k \pmod 4$. We denote the space of such forms $H^+_{k+\frac{1}{2}}(\Gamma_0(4N))$ (resp. $M^{+,!}_{k+\frac{1}{2}}(\Gamma_0(4N))$).

For odd N, there is a natural projection operator $|\,\mathrm{pr} : S_{k+\frac{1}{2}}(\Gamma_0(4N)) \to S^+_{k+\frac{1}{2}}(\Gamma_0(4N))$ given in terms of slash operators which extends to spaces of weakly holomorphic modular forms and harmonic Maaß forms. Let $f \in M^{!,+}_{k+\frac{1}{2}}(\Gamma_0(4N))$, where N is an odd integer. Then the projection operator acts on f in the following way [37] (see also [31])

$$(f|\,\mathrm{pr})(\tau) = (-1)^{\lfloor \frac{k+1}{2} \rfloor} \frac{1}{3\sqrt{2}} \sum_{v=-1}^{2} \left(f| \left(\begin{smallmatrix} 4(1+Nv) & 1 \\ 8Nv & 4 \end{smallmatrix} \right) \right)(\tau) + \frac{1}{3} f(\tau). \tag{2.15}$$

The action of this projection operator on principal parts of harmonic Maaß forms is described in the following lemma (see [31, Lemma 2.9, 2.10] and [24, Lemma 2.6]).

Lemma 2.6. *Let N be odd and $f \in H_{k+\frac{1}{2}}(\Gamma_0(4N))$ for some $k \in \mathbb{N}$, such that*

$$f^+(\tau) = q^{-m} + \sum_{n=0}^{\infty} a_n q^n \tag{2.16}$$

for some $m > 0$ with $-m \equiv 0, (-1)^k \pmod 4$, and suppose that f has a non-vanishing principal part only at the cusp ∞ and is bounded at the other cusps of $\Gamma_0(4N)$. Then the projection $f|\,\mathrm{pr}$ of f to the plus space has a pole of order m at ∞, a pole of order $\frac{m}{4}$ either at the cusp $\frac{1}{N}$ if $m \equiv 0 \pmod 4$ or at the cusp $\frac{1}{2N}$ if $-m \equiv (-1)^k \pmod 4$ and is bounded at all other cusps.

For even N, we have the following lemma for the Rademacher sums that we consider in this paper.

Lemma 2.7. *For even N, the Rademacher sum $R^{[-5]}_{\frac{3}{2},4N,\psi}(\tau)$ satisfies the Kohnen plus space condition.*

Proof. This is an immediate consequence of Lemma 2.10 of [31]. □

For even N, we define the projection operator $|\,\mathrm{pr}$ to be the following sieving operator: Let $f(\tau) = \sum_{n=n_0}^{\infty} c(n)q^n$ be modular of weight $k+\frac{1}{2}$ where $k \in \mathbb{N}$, and level $4N$, where N is even, then we define

$$f|\,\mathrm{pr} = \sum_{\substack{n=n_0 \\ n\equiv 0,(-1)^k \pmod 4}}^{\infty} c(n)q^n. \tag{2.17}$$

By Lemma 2.7, we have $R^{[-5]}_{\frac{3}{2},4N,\psi}(\tau)|\,\mathrm{pr} = R^{[-5]}_{\frac{3}{2},4N,\psi}(\tau)$ if N is even.

2.5. Eta-quotients

For the rational conjugacy classes $[g] \in \{21A, 30AB\}$, it is convenient to use eta-quotients instead of Rademacher sums.

Recall that an eta-quotient is defined to be a function of the form

$$f(\tau) = \prod_{\delta|N} \eta(\delta\tau)^{r_\delta}, \tag{2.18}$$

where $r_\delta \in \mathbb{Z}$ and $\eta(\tau) := q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n)$ is the Dedekind eta function. As a consequence of the product definition for $\eta(\tau)$, any eta-quotient is non-vanishing on $\mathbb{H}$. We will need the following lemma from [47] to construct eta-quotients which vanish only at a specific cusp.

Lemma 2.8. *([47, Lemma 14]) Let $N \in \mathbb{N}$, then for each divisor d of N, there exist $k_d \in \mathbb{N}$ and a corresponding eta-quotient $E_{d,N}(\tau) \in M_{k_d}(\Gamma_0(N))$ such that $E_{d,N}$ vanishes only at the cusp $\frac{c}{d}$.*

The proof of Lemma 2.8 is constructive, and MAGMA [5] code implementing it can be found at http://users.wfu.edu/rouseja/eta/. We write $E_N(\tau)$ for the holomorphic eta-quotient $E_{N,N}(\tau)$ that is produced by this code. In Section 3.2 we will use the explicit construction of eta-quotients $E_N(\tau)$ to construct weakly holomorphic modular forms $f_g^{wh}(\tau)$ for $[g] \in \{21A, 30AB\}$.

For completeness, we recall here the modular transformation law of the Dedekind eta-function,

$$\eta\left(\frac{az+b}{cz+d}\right) = e\left(\frac{a+d}{24c} + \frac{s(-d,c)}{2} + \frac{3}{8}\right)(cz+d)^{\frac{1}{2}}\eta(z). \tag{2.19}$$

Here, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $s(d,c)$ is the Dedekind sum,

$$s(d,c) = \sum_{r=1}^{c-1} \frac{r}{c}\left(\frac{dr}{c} - \left\lfloor \frac{dr}{c} \right\rfloor - \frac{1}{2}\right). \tag{2.20}$$

Using eq. (2.19), we can explicitly compute Fourier coefficients of $(f|_{k,\psi}\gamma)(\tau)$ whenever f is an eta-quotient, $\gamma \in \Gamma_0(N)$ and ψ is a multiplier system of weight k and level N.

3. McKay–Thompson series

To state our main theorem of this section, we associate to each rational conjugacy class $[g]$ of the Thompson group Th, the following data:

(1) Integers v_g and h_g as specified in Table A.1. We use these to define the character $\psi_g := \psi_{4|g|,v_g,h_g}$ (see Equation (2.3)), where $|g|$ denotes the order of g in Th.
(2) The space of cusp forms $S_g := S_{\frac{3}{2}}^{+}(\Gamma_0(4|g|), \psi_g)$ of weight $\frac{3}{2}$ in the plus-space which transform under $\Gamma_0(4|g|)$ with character ψ_g. We define d_g to be the dimension of this space and let f_g be the d_g-tuple $f_g := (f_g^{(1)}, \ldots, f_g^{(d_g)})$ where $f_g^{(i)}$ is the i^{th} element of the echelonized basis of S_g. A list of $f_g^{(i)}$'s can be found in Table A.3.
(3) For each $f_g^{(i)}$ defined as above, we let $n_g^{(i)}$ and $m_g^{(i)}$ be the integers listed in Table A.4. We define n_g to be the d_g-tuple $n_g := (n_g^{(1)}, \ldots, n_g^{(d_g)})$, and define M_g to be the $d_g \times d_g$ diagonal matrix with entries given by $(m_g^{(1)}, \ldots, m_g^{(d_g)})$.
(4) Finally, to each rational conjugacy class $[g]$ of Th, we associate integers $a_g(n)$ for each $n > 0$, where $n \equiv 0, 3 \pmod 4$. For $g \notin \{21A, 30AB\}$, the integers $a_g(n)$ are given by Equation (3.8). For $m \in \{21, 30\}$, we will prove in Lemma 3.4 that there exists a weakly holomorphic modular form in $M_{\frac{3}{2}}^{+,!}(\Gamma_0(4m), \psi_{mA})$ which has a pole of order 5 at ∞, a pole of order $\frac{5}{4}$ at the cusp $\frac{1}{42}$ if $m = 21$, and vanishes at all other cusps. For $g = 21A$ we let $f_{mA}^{wh}(\tau)$ denote the unique such form whose Fourier expansion begins $6q^{-5} - 2q^4 + 4q^7 - 8q^8 + O(q^{11})$, and we define $a_{21A}(n)$ by setting

$$f_{21A}^{wh} = 6q^{-5} + \sum_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}}^{\infty} a_{21A}(n)q^n. \tag{3.1}$$

Similarly, we define $a_{30AB}(n)$ to be the Fourier coefficients of $f_{30AB}^{wh} \in M_{\frac{3}{2}}^{+,!}(\Gamma_0(120), \psi_{30})$, which is the unique form satisfying all properties in Lemma 3.4 with the Fourier expansion $6q^{-5} + 3q^3 + 3q^8 - 3q^{11} + O(q^{12})$.

For each rational conjugacy class $[g]$ we define Λ_g to be the set of all d_g-tuples $\lambda_g := (\lambda_g^{(1)}, \dots, \lambda_g^{(d_g)}) \in \mathbb{Z}^{d_g}$ and obtain the following proposition.

Proposition 3.1. *Fix a rational conjugacy class $[g]$ in Th. Then for each $\lambda_g \in \Lambda_g$, the function*

$$\mathcal{F}_g^{\lambda}(\tau) := 6q^{-5} + \sum_{0<n} a_g(n)q^n + (\lambda_g M_g + n_g) \cdot f_g(\tau) \tag{3.2}$$

is a weakly holomorphic modular form that satisfies the following properties.

(a) *It lies in $M_{\frac{3}{2}}^{+,!}(\Gamma_0(4|g|), \psi_g)$, i.e., $\mathcal{F}_g^{\lambda}(\tau)$ has weight $\frac{3}{2}$, level $4|g|$ with character ψ_g, and satisfies the Kohnen plus space condition.*
(b) *It has a pole of order 5 at the cusp ∞, a pole of order $\frac{5}{4}$ at the cusp $\frac{1}{2|g|}$ if $|g|$ is odd, and vanishes at all other cusps.*
(c) *The Fourier coefficients of $\mathcal{F}_g^{\lambda}(\tau)$ are integers.*

Note that our multiplier system ψ_g is conjugate to the one used by [31] and [33]. This is necessary for Theorem 3.2 to be true, and is not unexpected since our functions are weight $\frac{3}{2}$ as opposed to the weight $\frac{1}{2}$ forms in [31] and [33].

We will prove Proposition 3.1 by constructing specific weakly holomorphic forms $f_g^{wh}(\tau) = 6q^{-5} + \sum_{0<n} a_g(n) \in M_{\frac{3}{2}}^{+,!}(\Gamma_0(4|g|), \psi_g)$ using the theory of Rademacher sums and eta-quotients. We will see from the explicit construction that each $f_g^{wh}(\tau)$ already satisfies properties $(a) - (c)$ listed in Proposition 3.1 even without the addition of any cusp forms. We need to add the cusp forms $f_g(\tau)$ not for Proposition 3.1, but instead for the following theorem.

Theorem 3.2. *Assume the above notation and let Λ be the set of functions $\{\lambda : g \mapsto \lambda_g \in \Lambda_g\}$. Then, for each $\lambda \in \Lambda$, there exists an infinite-dimensional graded virtual Th-module*

$$W^{\lambda} := \bigoplus_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}} W_n^{\lambda} \tag{3.3}$$

such that for each rational conjugacy class $[g]$ of Th, the corresponding McKay–Thompson series,

$$6q^{-5} + \sum_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}} \operatorname{tr}\left(g|W_n^{\lambda}\right) q^n \tag{3.4}$$

is the specific weakly holomorphic modular form $\mathcal{F}_g^{\lambda}(\tau) \in M_{\frac{3}{2}}^{+,!}(\Gamma_0(4|g|), \psi_g)$ *described in Proposition 3.1. Furthermore, for every infinite-dimensional graded virtual Th-module* $W = \bigoplus_{n>0} W_n$ *for which the McKay–Thompson series,*

$$\mathcal{F}_g(\tau) = 6q^{-5} + \sum_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}} \operatorname{tr}\left(g|W_n\right) q^n \tag{3.5}$$

satisfies the properties listed in Proposition 3.1, there exists a $\lambda \in \Lambda$ *for which* $W = W^{\lambda}$ *described as above.*

We will now construct the relevant spaces of modular forms required for the proof of Proposition 3.1.

3.1. Using Rademacher sums

For each rational conjugacy class $[g] \notin \{21A, 30AB\}$, consider the function

$$f_g^{wh}(\tau) = 6R^{[-5],+}_{\frac{3}{2},4|g|,\psi_g}(\tau) := 6\left(R^{[-5]}_{\frac{3}{2},4|g|,\psi_g}|\operatorname{pr}\right)(\tau) \tag{3.6}$$

where $|\operatorname{pr}$ is the projection onto the Kohnen plus-space (see Section 2.4). Then by Lemma 2.5, Lemma 2.6 and Lemma 2.7, each $f_g^{wh}(\tau)$ is a mock modular form in the plus-space of weight $\frac{3}{2}$, level $|g|$, and multiplier ψ_g, has a pole of order 5 at the cusp at infinity, a pole of order $\frac{5}{4}$ at the cusp $\frac{1}{2|g|}$ if $|g|$ is odd (forced by the projection to the plus-space, see Lemma 2.6), and vanishes at all other cusps. The only thing left to prove here is that each $f_g^{wh}(\tau)$ is, in fact, weakly holomorphic (i.e., has vanishing shadow, see Proposition 2.4).

Lemma 3.3. *For each rational conjugacy class* $[g] \notin \{21A, 30AB\}$ *of the Thompson group, the function* $f_g^{wh}(\tau)$ *(defined in eq. (3.6)) is in fact a weakly holomorphic modular form, and has Fourier expansion given by*

$$f_g^{wh}(\tau) = 6q^{-5} + \sum_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}}^{\infty} a_g(n) q^n, \tag{3.7}$$

where for $N = |g|$*, we have*

$$a_g(n) := \frac{-3\pi}{N}\left(\frac{-n}{5}\right)^{\frac{1}{4}} \sum_{c=1}^{\infty} \frac{1+\delta_{\text{odd}}(Nc)}{c} K_{\frac{3}{2},\psi}(-5, n, 4Nc) I_{\frac{1}{2}}\left(\frac{\pi\sqrt{5n}}{Nc}\right). \tag{3.8}$$

Here, $I_{\frac{1}{2}}$ is the modified Bessel function of the first kind of order $\frac{1}{2}$,

$$\delta_{\text{odd}}(k) := \begin{cases} 1 & k \text{ odd}, \\ 0 & k \text{ even}, \end{cases} \tag{3.9}$$

and $K_{\frac{3}{2},\psi}$ is the twisted Kloosterman sum

$$K_{\frac{3}{2},\psi}(m,n,c) := \sum_{d \pmod c} \psi\left(\left(\begin{smallmatrix} * & * \\ c & d \end{smallmatrix}\right)\right) \left(\frac{c}{d}\right) \varepsilon_d^3 e\left(\frac{m\bar{d}+nd}{c}\right). \tag{3.10}$$

The sum here runs over primitive residue classes modulo c, and $\bar{d}$ denotes the multiplicative inverse of d modulo c.

Proof. We have already established that each $f_g^{wh}(\tau)$ is a mock modular form of weight $\frac{3}{2}$ for the group $\Gamma_0(4|g|, \psi_g)$. It suffices to show that $f_g^{wh}(\tau)$ has vanishing shadow. By Proposition 2.4, the space of possible shadows is $M_{\frac{1}{2}}(\Gamma_0(4|g|), \overline{\psi_g}) \subset M_{\frac{1}{2}}(\Gamma_0(4|g|h_g))$. By the Serre-Stark basis theorem [49] (see also [42, Theorem 1.45]), the (*a priori*) larger space is generated by theta functions of the form $\theta_\chi(k\tau) = \sum_{n\in\mathbb{Z}} \chi(n) q^{kn^2}$, where χ is an even Dirichlet character and χ and k depend on $N = |g|$. We compute the Bruinier-Funke pairing [8] to deduce that

$$\{\widehat{f_g^{wh}(\tau)}, \theta_\chi(k\tau)\} \neq 0 \tag{3.11}$$

if and only if $k = 5$. Thus, the only way to get non-vanishing shadow would be if the shadow is a constant multiple of $\theta_\chi(5\tau)$ but by Lemma 2.5, the shadow is in fact a constant multiple of the Rademacher sum $R^{[+5]}_{\frac{1}{2},4N,\overline{\psi_g}}(\tau)$. Since they transform under $\Gamma_0(4|g|)$ with different characters, this is not possible.

Thus, each $f_g^{wh}(\tau)$ has vanishing shadow and is in fact weakly holomorphic. Computing the coefficients of Rademacher sums in terms of Kloosterman sums and Bessel functions is a standard computation, see for example [11] (or Proposition 2.7 in [24]). □

3.2. Using eta-quotients

For $[g] \in \{21A, 30AB\}$, we will use the eta-quotients $E_{|g|}(\tau)$ in Lemma 2.8 to compute spaces of weakly holomorphic forms of the desired weight and level. The main result of this section is the following lemma.

Lemma 3.4. *For $m \in \{21, 30\}$, there exists a weakly holomorphic modular form with integer Fourier coefficients in $M^{!,+}_{\frac{3}{2}}(\Gamma_0(4m, \psi_{mA}))$ which has a pole of order 5 at ∞, a pole of order $\frac{5}{4}$ at the cusp $\frac{1}{42}$ if $m = 21$, and vanishes at all other cusps.*

Note that if Lemma 3.4 is true, such a form satisfies all properties of Proposition 3.1, and we can thus define $f^{wh}_{21A}(\tau)$ (resp. $f^{wh}_{30AB}(\tau)$) to be the unique such form with Fourier expansion $6q^{-5} - 2q^4 + 4q^7 - 8q^8 + O(q^{11})$ (resp. $6q^{-5} + 3q^3 + 3q^8 - 3q^{11} + O(q^{12})$).

Remark. We could have written an analogous statement for each rational conjugacy class $[g]$ in the Thompson group and forgone the discussion about Rademacher sums completely. This would not affect the proof of Theorem 3.2 at all. However, we need an expression for $f^{wh}_g(\tau)$ for certain classes $[g] \notin \{21A, 30B\}$ in terms of Rademacher sums for the application to elliptic curves. In particular, such expressions for $g \in \{14A, 19A\}$ play key roles in the proofs of Theorems 1.1 and 1.3. On the other hand, for $g \in \{21A, 30AB\}$, the analogue of the sum in Equation (3.8) converges very slowly, so it is more convenient to use eta-quotients instead of Rademacher sums in these cases.

Proof of Lemma 3.4. By Lemma 2.8, for each $N > 0$ we can construct an eta-quotient $E_N(\tau)$ that vanishes only at the cusp ∞. We use $N = 21$ and $N = 30$ to get eta-quotients:

$$E_{21}(\tau) = \frac{\eta(\tau)\eta(21\tau)^{21}}{\eta(3\tau)^3\eta(7\tau)^7} \quad \text{and} \quad E_{30}(\tau) = \frac{\eta(2\tau)^2\eta(3\tau)^3\eta(5\tau)^5\eta(30\tau)^{30}}{\eta(\tau)\eta(6\tau)^6\eta(10\tau)^{10}\eta(15\tau)^{15}} \tag{3.12}$$

of weight 6 and 4, respectively. Now, consider the cusp form space $S_{\frac{15}{2}}(\Gamma_0(84), \psi_{21A})$, and suppose for now that we can compute a basis for this space explicitly. If so, we can divide each element of the basis by $E_{21}(4\tau)$ to get a generating set B_{21} of forms in $M^!_{\frac{3}{2}}(\Gamma_0(84), \psi_{21A})$ whose only (possible) pole is at the cusp ∞. Then, we apply the projection operator to each element of B_{21} to get a generating set of forms in $M^{!,+}_{\frac{3}{2}}(\Gamma_0(84), \psi_{21A})$ that are holomorphic away from the cusps at ∞ and $\frac{1}{42}$. This generating set turns out to be non-empty.

We can now construct $f^{wh}_{21A}(\tau)$ as a suitable linear combination of elements of this space determined completely by its Fourier expansion $6q^{-5} - 2q^4 + 4q^7 - 8q^8 + O(q^{11})$. The same argument works for $f^{wh}_{30AB}(\tau)$ if we start with $S_{\frac{11}{2}}(\Gamma_0(120), \psi_{30AB})$ instead. Here again, the set of forms in $M^{!,+}_{\frac{3}{2}}(\Gamma_0(120), \psi_{30AB})$ which are holomorphic away from the cusp at ∞ turns out to be non-empty.

We now describe how to compute the bases for $S_{\frac{15}{2}}(\Gamma_0(84), \psi_{21A})$ and $S_{\frac{11}{2}}(\Gamma_0(120), \psi_{30AB})$ in some detail. We will essentially follow the method described in Proposition 3.1 of [31]. Let $(m, k) \in \{(21, \frac{15}{2}), (30, \frac{11}{2})\}$. Let $f \in S_k(\Gamma_0(4m)), \psi_{mA})$ and let

$$\vartheta(\tau) := \sum_{n \in \mathbb{Z}} q^{n^2} \in M^+_{\frac{1}{2}}(\Gamma_0(4)). \tag{3.13}$$

Then $f\vartheta$ lies in $M_{k+\frac{1}{2}}(\Gamma_0(4m), \psi_{mA}) \subset M_{k+\frac{1}{2}}(\Gamma_0(4mh_g))$. Using programs (available at http://users.wfu.edu/rouseja/eta/) written by Rouse and Webb one can verify that the space $M_{k+\frac{1}{2}}(\Gamma_0(12m))$ is generated by eta quotients ($h_g = 3$, for both values of m). Since we can explicitly compute Fourier expansions of $(g|_k\gamma)(\tau)$ for any eta-quotient $g(\tau)$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ (see Section 2.5), we can thus compute a basis for

$M_{k+\frac{1}{2}}(\Gamma_0(4m), \psi_{mA})$ and hence for $S_k(\Gamma_0(4m)), \psi_{mA})$. Alternatively, we can also compute a basis for $M_{k+\frac{1}{2}}(\Gamma_0(4m), \psi_{mA})$ using in-built functions in PARI/GP [44]. This concludes the proof of Lemma 3.4. □

We now have an explicit description of $f_g^{wh}(\tau)$ for each rational conjugacy class $[g]$. The next steps in the proof are showing that each $f_g^{wh}(\tau)$ (and thus each $\mathcal{F}_g^{\lambda}(\tau)$) satisfies all properties listed in Proposition 3.1 (we do this in Section 3.3), and that the only cusp forms we can add for Theorem 3.2 to be true are appropriate integer multiples of the elements of S_g for each $g \in Th$, respectively (cf. Proposition 3.1). The latter will follow from our work in Section 4.

3.3. Cusp forms

We begin by noting that the weakly holomorphic forms $f_g^{wh}(\tau)$ described in Sections 3.1 and 3.2 satisfy the properties $(a) - (c)$ listed in Proposition 3.1. Also, said properties uniquely determine a weakly holomorphic form up to cusp forms [24, Lemma 2.4]. Thus to specify the functions $\mathcal{F}_g^{\lambda}(\tau)$ completely we have to compute the cusp form spaces $S_{\frac{3}{2}}^{+}(\Gamma_0(4|g|), \psi_g)$ for each $[g]$ in Th.

Lemma 3.5. *For each rational conjugacy class $[g]$ of Th, the corresponding cusp form space S_g is spanned by the cusp forms given in Table A.3.*

Proof. We use the same method as in the proof of Lemma 3.4 to compute the cusp form spaces. Let $f \in S_{\frac{3}{2}}^{+}(4|g|, \psi_g)$ be any cusp form. Then $f\vartheta$ lies in $M_2(4|g|, \psi_g) \subset M_2(4|g|h_g)$, where the larger space is spanned by eta quotients for each $[g]$. This can be verified using `MAGMA` code written by Rouse and Webb [47]. We can then use the modular properties of the eta-quotients and the projection onto the plus-space to determine a basis for $M_2(4|g|, \psi_g)$ and hence $S_g = S_{\frac{3}{2}}^{+}(4|g|, \psi_g)$. The space S_g turns out to be trivial for every

$$[g] \notin \{12D, 14A, 18B, 19A, 20A, 21A, 24AB, 24CD, 28A, 30AB, 31AB, 39AB\}. \quad (3.14)$$

The Fourier coefficients given in Table A.3 are enough to determine each $f_g^{(i)}(\tau)$ completely for all other rational conjugacy classes $[g]$. □

3.4. Integer coefficients

The last thing we need to check in order to prove Proposition 3.1 is that the functions

$$\mathcal{F}_g^{\lambda}(\tau) = f_g^{wh}(\tau) + (\lambda_g M_g + n_g) \cdot f_g(\tau) \quad (3.15)$$

constructed in the preceding section have integer coefficients. We will use Sturm's theorem [54] for this. Note that each of these functions lies in $M_{\frac{3}{2}}^{+,!}(\Gamma_0(4|g|), \psi_g) \subset$

$M^{+,!}_{\frac{3}{2}}(\Gamma_0(4|g|h_g))$, thus if $\nu(\tau) = q^5 + O(q^8)$ is a cusp form with integer coefficients in $S^{+}_{2k-\frac{3}{2}}(\Gamma_0(4|g|h_g))$, then, $\mathcal{F}_g^{\lambda}(\tau)\nu(\tau)$ lies in $M_{2k}(\Gamma_0(4|g|h_g))$, so we can apply Sturm's theorem to it. Thus, $\mathcal{F}_g^{\lambda}(\tau)$ has integer coefficients if the first $\frac{k}{6}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4|g|h_g)]$ coefficients of $\mathcal{F}_g^{\lambda}(\tau)\nu(\tau)$ are integers. The largest bound we have to check is less than 1200. The author used PARI/GP [44] to do this computation.

This concludes the proof of Proposition 3.1.

4. Proof of Theorem 3.2: integer multiplicities

To prove Theorem 3.2, we have to show that the $\mathcal{F}_g^{\lambda}(\tau)$'s we described in Section 3 are indeed the McKay–Thompson series of a virtual module of the Thompson group.

This is equivalent to proving that there exist integers $m_1^{\lambda}(n), ..., m_{39}^{\lambda}(n)$ such that if $\mathcal{F}_g^{\lambda}(\tau) = 6q^{-5} + \sum_{n\geq 3} \alpha_g^{\lambda}(n)q^n$, then for each $n \geq 3$ the Fourier coefficient $\alpha_g^{\lambda}(n)$ can be written in the form,

$$\alpha_g^{\lambda}(n) = \sum_{j=1}^{39} m_j^{\lambda}(n)\chi_j(g), \tag{4.1}$$

where $\chi_1, \ldots, \chi_{39}$ are the irreducible rational characters of Th (see Section 2.1 for a definition of rational character). We say that the function $\omega_n^{\lambda} : Th \to \mathbb{C}$, defined by $g \mapsto \alpha_g^{\lambda}(n)$, is a *virtual rational character* of Th if the above condition is satisfied. Thus, the goal of this section is to prove that ω_n^{λ} is a virtual rational character of Th for every $n \geq 3$ and choice of $\lambda \in \Lambda$.

As explained in [31], this is computationally infeasible to prove directly using only Sturm bounds [54]. However, it can be reduced to a finite computation using a variant of Thompson's reformulation (see, for example, [53]) of Brauer's characterization of generalized characters. (For another example of a similar computation, see [29].) To state the result, we first have to define a few things.

For the rest of this section, let G be a finite group and p a fixed prime dividing the order of G. Let $\mathscr{C}_G$ denote the set of all rational conjugacy classes of G. We call $[g] \in \mathscr{C}_G$ *p-regular* if the order of g is coprime to p. Let K_p denote the set of all p-regular classes in G whose centralizer in G has order divisible by p. For a fixed $[g] \in K_p$, we will let α denote the highest power of p dividing the order of the centralizer of g in G. (This α should not be confused with the $\alpha_g^{\lambda}(n)$ of eq. (4.1).)

Let $h \in G$ be any element in G and let $|h| = n = p^k m$ where $k \geq 0$ and $(p, m) = 1$. Then we can write h as a product $h = ab$, where a and b commute and a has order m. (Both a and b can be expressed as powers of h.) We call a the *p-regular part* of h. We note here that if $h' \in G$ is in the same rational conjugacy class as h, then their corresponding p-regular parts a' and a are also in the same rational conjugacy class, i.e. if $h' \in [h]$ then $a' \in [a]$. This allows us to make the following definition.

Definition 4.1. For a fixed p and $[g] \in K_p$ as above, the *p-regular section* $R_{p,g}$ of $[g]$ is the set of rational conjugacy classes $[h] \in \mathscr{C}_G$ such that the p-regular part of h lies in $[g]$.

For $G = Th$, and for each prime p dividing $|G|$, Table A.2 lists the rational conjugacy classes $[g]$ in K_p, along with their p-regular section $R_{p,g}$ and the highest power α such that p^α divides the order of the centralizer $C_G(g)$.

For a fixed group G, and prime p dividing $|G|$, fix a rational conjugacy class $[g] \in K_p$. Let $\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b\}$ denote the localization of $\mathbb{Z}$ at the prime ideal (p), and let $I := p^\alpha \mathbb{Z}_{(p)}$. We define $m := |R_{p,g}|$, and let $M_{p,g}$ denote the set of all m-tuples $(l_1, l_2, \ldots, l_m) \in \mathbb{Z}_{(p)}^{\oplus m}$ such that

$$\sum_{i=1}^{m} l_i \chi([h]_i) \equiv 0 \pmod{I^m} \tag{4.2}$$

for all irreducible rational characters χ of G and all rational conjugacy classes $[h]_i$ in $R_{p,g}$.

We are now ready to state the following important lemma.

Lemma 4.2. *Assuming the above notation, an integer-valued class function $c : G \to \mathbb{Z}$ of G is a virtual rational character of G if and only if for all primes p and rational conjugacy classes $[g]$,*

$$\sum_{i=1}^{m} l_i c([h]_i) \equiv 0 \pmod{I^m} \tag{4.3}$$

for all $(l_1, l_2, \ldots, l_m) \in M_{p,g}$.

Proof. This is a direct application of [53, Theorem 1.1]. □

Lemma 4.2 reduces the problem of checking whether the multiplicities are integral to a p-local computation. We illustrate this with an example.

Example 1. Let $p = 19$. Then, $K_{19} = \{1A\}$ and $R_{19,1A} = \{1A, 19A\}$. We have $\alpha = 1$, and $M_{19,1A}$ is the set of ordered pairs $(x, y) \in \mathbb{Z}_{(19)}^{\oplus 2}$ such that

$$x\chi(1A) + y\chi(19A) \equiv 0 \pmod{19} \tag{4.4}$$

for each irreducible rational character χ of the Thompson group. Plugging in values for $\chi(1A)$ and $\chi(19A)$, we find that $M_{19,1A} = \{(x, y) \in \mathbb{Z}_{(19)}^{\oplus 2} \mid x + y \equiv 0 \pmod{19}\}$. So in order to prove that $\omega_n^\lambda : Th \to \mathbb{C}$ is a virtual rational character for each $\lambda \in \Lambda$ and $n \in \mathbb{Z}$, we need to check that for each $(x, y) \in M_{19,1A}$,

$$x\alpha_{1A}^\lambda(n) + y\alpha_{19A}^\lambda(n) \equiv 0 \pmod{19} \tag{4.5}$$

where $\mathcal{F}_g^\lambda(\tau) = 6q^{-5} + \sum_{n\geq 3} \alpha_g^\lambda(n)$ (cf. eq. (4.1)). Thus, we have to show that the following congruence is satisfied for every $n \in \mathbb{N}$ and $\lambda \in \Lambda$

$$\alpha_{1A}^\lambda(n) - \alpha_{19A}^\lambda(n) \equiv 0 \pmod{19}. \tag{4.6}$$

This is a doubly infinite set of congruences (for each fixed $\lambda \in \Lambda$, we have a congruence for every integer n), but we can get rid of the dependence on λ as follows: Note that $\alpha_{1A}^\lambda(n)$ is independent of λ since the cusp form space S_{1A} is empty so we can write $a_{1A}(n)$ for $\alpha_{1A}^\lambda(n)$ (see Proposition 3.1 for notation). Also by Proposition 3.1, $\alpha_{19A}^\lambda(n) = a_{19A}(n) + (m_{19A}\lambda_{19A} + n_{19A})b_{19A}(n)$ where $b_{19A}(n)$ is the n^{th} coefficient of $f_{19A}(\tau) \in S_{19A}$. From Table A.4, $m_{19A} = 18$ and $n_{19A} = 19$, so checking eq. (4.6) reduces to checking that

$$a_{1A}(n) = a_{19A}(n) + 18b_{19A}(n) \pmod{19} \tag{4.7}$$

for all $n \in N$.

We can do the same thing for every pair $(p, [g])$ where $[g] \in K_p$, and get a list of congruences that we need to check in order to show that the function ω_n^λ is a virtual rational character in every case. An inspection of Table A.4 and Table A.3 confirms that we can always get rid of the dependence on λ. This still isn't a finite computation because at the moment, we need to check each congruence for all positive integers n. However, that can be easily resolved in the following way: Let $\upsilon(\tau)$ be the unique cusp form in $S^+_{\frac{37}{2}}(\Gamma_0(4))$ whose Fourier expansion is of the form $q^5 - 56q^8 + O(q^9)$. Then for each $[g]$ and λ, $\mathcal{F}_g^\lambda(\tau)\upsilon(\tau)$ is a holomorphic modular form of weight 20 and level $|g|h_g$ so Sturm's theorem [54] applies. Thus, it suffices to check that the congruences hold for the first M Fourier coefficients of the holomorphic modular form where M is the Sturm bound which in the worst case is just shy of 4000. As before, we used [44] to check these.

We conclude this section with another example of this procedure, for clarity.

Example 2. Let $p = 3$, then $K_3 = \{1A, 2A, 4A, 4B, 5A, 7A, 8A, 8B, 10A, 13A\}$. Pick $[g] = 1A$. Then, $\alpha = 10$, $R_{p,g} = \{1A, 3A, 3B, 3C, 9A, 9B, 9C, 27A, 27BC\}$ and $M_{3,1A}$ is the set of 9-tuples $(y_1, y_2, \ldots, y_9)$ in $\mathbb{Z}_{(3)}^{\oplus 9}$ such that

$$y_1\chi(1A) + y_2\chi(3A) + \cdots + y_9\chi(27BC) \equiv 0 \pmod{3^{10}}$$

for each irreducible rational character χ of the Thompson group. As before, in order to prove that $\omega_n^\lambda : Th \to \mathbb{C}$ is a virtual rational character for each $\lambda \in \Lambda$ and $n \in \mathbb{Z}$, we need to check that for each $(y_1, \ldots, y_9) \in M_{3,1A}$ we have,

$$y_1\alpha_{1A}^\lambda + y_2\alpha_{3A}^\lambda + \cdots + y_9\alpha_{27BC}^\lambda \equiv 0 \pmod{3^{10}}. \tag{4.8}$$

This is easier to manage as a matrix computation. We let X denote the 39×9 matrix

$$X = [\chi_i(h)]_{0<i\leq 39, h\in R_{p,g}},$$

and let $\mathbf{a} := (a_{1A}, a_{3A}, a_{3B}, \ldots, a_{27BC})$. For each $(y_1, \ldots, y_9) \in M_{3,1A}$, we denote by $\mathbf{y}$ the corresponding column vector whose entries are $y_1, y_2, \ldots, y_9$.

Note that for all rational conjugacy classes $[g]$ in $R_{3,1A}$ the corresponding cusp form space S_g is empty, so we can in fact reduce to checking that $\mathbf{a} \cdot \mathbf{y} \equiv 0 \pmod{3^{10}}$ for all $\mathbf{y}$ such that $X\mathbf{y} \equiv 0 \pmod{3^{10}}$. In order to check this, we first compute a basis for the $\mathbb{Z}_{(3)}$-span of the row vectors of X. We can use the `GAP` [30] command `BaseIntMat` to do this computation. It turns out that the $\mathbb{Z}_{(3)}$-span of the row vectors of X is the same as that of the row vectors of the following 9×9 matrix:

$$M := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 9 & 1944 & 72 & 0 & 45 & 24 & 0 & 15 \\ 0 & 0 & 2187 & 0 & 0 & 27 & 0 & 3 & 3 \\ 0 & 0 & 0 & 81 & 0 & 27 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 27 & 27 & 0 & 3 & 3 \\ 0 & 0 & 0 & 0 & 0 & 81 & 9 & 6 & 15 \\ 0 & 0 & 0 & 0 & 0 & 0 & 27 & 0 & 18 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9 & 9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 27 \end{bmatrix}. \tag{4.9}$$

We can solve $M\mathbf{y} \equiv 0 \pmod{3^{10}}$ for $\mathbf{y}$ and then compute $\mathbf{a}.\mathbf{y}$ modulo 3^{10} to see that the congruences we need to check are:

$$\begin{aligned} a_{1A} - a_{3A} &\equiv 0 \pmod{3^2} \\ a_{1A} - a_{9A} &\equiv 0 \pmod{3^3} \\ 7a_{1A} - 8a_{3A} + a_{3C} &\equiv 0 \pmod{3^4} \\ 215a_{1A} - 216a_{3A} + a_{3B} &\equiv 0 \pmod{3^7} \\ a_{1A} + 27a_{3A} - a_{3B} - 27a_{3C} - 81a_{9A} + 81a_{9B} &\equiv 0 \pmod{3^8} \\ 1214a_{1A} - 1971a_{3A} + a_{3B} + 27a_{3C} + 81a_{9A} - 81a_{9B} + 729a_{9C} &\equiv 0 \pmod{3^9} \\ 2591a_{1A} - 594a_{3A} + a_{3B} - 54a_{3C} + 81a_{9A} + 162a_{9B} - 2187a_{27A} &\equiv 0 \pmod{3^9} \\ 1214a_{1A} + 216a_{3A} + a_{3B} + 27a_{3C} + 81a_{9A} - 81a_{9B} - 1458a_{9C} + \ldots & \\ -2187a_{27A} + 2187a_{27BC} &\equiv 0 \pmod{3^{10}}. \end{aligned} \tag{4.10}$$

(Alternatively, we can use GAP to check that any given vector $\mathbf{a}$ is in the aforementioned span, by using the following code: `IsContainedInSpan(MutableBasis(Integers, M),a mod` 3^{10}`)`.)

As in Example 1, we can use PARI [44] to check these congruences up to the Sturm bound, which in this case comes out to be less than 1100.

We can continue in this manner and check that all multiplicities are integral and hence for each $\mathcal{F}_g^\lambda(\tau)$ as described in Proposition 3.1, there exists a virtual Th-module W^λ such that for each $[g]$ in Th,

$$\mathcal{F}_g^\lambda(\tau) = 6q^{-5} + \sum_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}} \operatorname{tr}\left(g|W_n^\lambda\right) q^n \tag{4.11}$$

This proves Theorem 3.2.

5. Elliptic curves

The family of Th-modules that we get from Theorem 3.2 encodes arithmetic information about quadratic twists of elliptic curves with conductors 14 and 19. This is the content of Theorems 1.1 and 1.3. We will prove these theorems in this section, but first, we have to develop some background. We recall here some basic notation and facts about traces of singular moduli, which were studied by Zagier in [64] and have since been examined extensively.

5.1. Traces of singular moduli

Let $\mathcal{Q}_D^{(N)}$ be the set of positive definite quadratic forms $Q = [a,b,c] := ax^2+bxy+cy^2$ of discriminant $-D = b^2-4ac < 0$ such that $N|a$. Then, $\Gamma_0(N)$ acts on $\mathcal{Q}_D^N$ with finitely many orbits. For $Q = [a,b,c] \in \mathcal{Q}_D^{(N)}$, we denote by $\tau_Q := \frac{-b+i\sqrt{D}}{2a}$ the unique root of $Q(x,1)$ in the upper half-plane $\mathbb{H}$. Let $f : \mathbb{H} \to \mathbb{C}$ be a function invariant under the action of $\Gamma_0(N)$, and $n \equiv 0,3 \pmod 4$ be a positive integer. Then we can define,

$$\operatorname{Tr}_D^{(N)}(f;n) := \sum_{Q\in \mathcal{Q}_{nD}^{(N)}/\Gamma_0(N)} \chi_D(Q)\frac{f(\tau_Q)}{\omega^{(N)}(Q)}, \tag{5.1}$$

where $\omega^{(N)}(Q)$ is the order of the stabilizer of Q in $\Gamma_0(N)/\{\pm 1\}$ and $\chi_D(Q)$ is the genus character for positive definite binary quadratic forms whose discriminants are multiples of D, defined as follows (see for example [39]):

$$\chi_D([a,b,c]) = \begin{cases} 0 & \text{if } (a,b,c,D) > 1 \\ \left(\frac{D}{r}\right) & \text{if } (a,b,c,D) = 1 \text{ and } Q \text{ represents } r \text{ with } (r,D) = 1. \end{cases} \tag{5.2}$$

For $N \in \{14,19\}$, let $J^{(N,+)}$ be the normalized Hauptmodul for the group $\Gamma_0^+(N)$. (We know this exists because the corresponding modular curve $X_0^{(+)}(N)$ has genus 0. See [27], or [24, Table 5.2].)

Proposition 5.1. *Let $N \in \{14, 19\}$ and let $J^{(N,+)}$ as above. Then,*

$$R^{[-5],+}_{\frac{3}{2},4N}(\tau) = q^{-5} + \frac{-2}{3\sqrt{5}} \sum_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}} \mathrm{Tr}^{(N)}_5(J^{(N,+)}; n)q^n \tag{5.3}$$

Proof. This is a direct application of Corollary 1.3 of [39]. □

In particular, this means that $f^{wh}_g(\tau)$ for $o(g) = N \in \{14, 19\}$ is given by

$$f^{wh}_g(\tau) = 6q^{-5} + \sum_{0<n} a_g(n)q^n = 6q^{-5} - \frac{4}{\sqrt{5}} \sum_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}} \mathrm{Tr}^{(N)}_5(J^{(N,+)}; n)q^n. \tag{5.4}$$

Writing $f^{wh}_g(\tau)$ in the above form turns out to be essential for the proofs of Theorems 1.1 and 1.3. We give here another key lemma which we will use in both proofs.

Lemma 5.2. *Let $N \in \{14, 19\}$ and let $d < 0$ be a fundamental discriminant that satisfies the respective conditions of Theorems 1.1 and 1.3; then*

$$\mathrm{Tr}^{(N)}_5(f, |d|) = 0 \tag{5.5}$$

for any $\Gamma_0(N)$ invariant function f, and hence, in particular, for $f = J^{(N,+)}(\tau)$.

Proof. For $N \in \{14, 19\}$, the conditions of the theorems ensure that $5d$ is not a square mod $4N$, which means that there are no quadratic forms $[a, b, c]$ of discriminant $b^2 - 4ac = 5d$ such that $N|a$. Thus $\mathcal{Q}^{(N)}_{|5d|}$ is empty for all such d and thus

$$\mathrm{Tr}^{(N)}_5(f; |d|) = \sum_{Q \in \mathcal{Q}^{(N)}_{|5d|}/\Gamma_0(N)} \chi_5(Q) \frac{f(\tau_Q)}{\omega^{(N)}(Q)} = 0 \tag{5.6}$$

for any function f that is $\Gamma_0(N)$ invariant. □

We now recall facts about elliptic curves that we will use in order to prove Theorems 1.1 and 1.3.

5.2. Elliptic curves

To prove our main results, we let E be an elliptic curve over $\mathbb{Q}$. For $d < 0$ a fundamental discriminant, we let E^d denote the d^{th} quadratic twist of E. We let N denote the conductor, $\Omega(E)$ denote the real period and $\mathrm{Reg}(E)$ denote the regulator of E. We refer the reader to standard texts on elliptic curves, e.g. [50] for the definitions of these invariants.

We let $L_E(s)$ denote the L-function associated to E. Then, by the modularity theorem [6] (see also [62,56]), there exists a unique weight 2 newform $\mathscr{G}_E = \sum_{n=1}^{\infty} a_E(n)q^n$ of level equal to the conductor of E such that

$$L_E(s) = \sum_{n=1}^{\infty} a_E(n)n^{-s}, \tag{5.7}$$

where the right-hand side extends to a holomorphic function on $\mathbb{C}$ [2]. We let $g_E(\tau) = \sum_{n=3}^{\infty} b_E(n)q^n \in S^+_{\frac{3}{2}}(\Gamma_0(4N))$ be the weight $\frac{3}{2}$ cusp form associated to $\mathscr{G}_E$ under the Shintani lift (see [34] for an overview of the Shintani lift). For $N \in \{14, 19\}$ the dimension of $S^+_{\frac{3}{2}}(\Gamma_0(4N))$ is 1, so for an elliptic curve of conductor N, the weight $\frac{3}{2}$ cusp forms $g_E(\tau)$ defined as above are the same as the cusp form $f_g(\tau)$ associated to $g \in \{14A, 19A\}$ in Section 3. This is the key fact that we employ in order to prove Theorems 1.1 and 1.3.

Let $E/\mathbb{Q}$ be an elliptic curve with square-free conductor N, and for each $\ell|N$, let ω_ℓ denote the eigenvalue of the newform $\mathscr{G}_E \in S_2(\Gamma_0(N))$ associated to E and the Atkin–Lehner involution W_ℓ.

Then we have the following lemma of Duncan, Mertens, and Ono, [24] (based on results due to Agashe [1] and Kohnen [37], and the generalization of Kohnen's work by Ueda and Yamana [60,61]) which connects the p-divisibility of the cusp form coefficient to $L_{E^d}(1)$.

Lemma 5.3. *(See [24, Lemma 6.5].) Assume the notation above, and let $p \geq 3$ be a prime. Let $d < 0$ be a fundamental discriminant satisfying $\left(\frac{d}{\ell}\right) = \omega_\ell$ for each ℓ. Denote by d_0 the smallest such discriminant. Then we have that*

$$\operatorname{ord}_p\left(\frac{L_{E^d}(1)}{\Omega(E^d)}\right) = \operatorname{ord}_p\left(\frac{L_{E^{d_0}}(1)}{\Omega(E^{d_0})}\right) + \operatorname{ord}_p\left(b_E(|d|)^2\right), \tag{5.8}$$

where E^d denotes the d^{th} quadratic twist of E.

Both our proofs of Theorems 1.1 and 1.3 depend on the above lemma. We are now ready to prove Theorem 1.1.

5.3. Proof of Theorem 1.1

Fix $W = W^\lambda$ to be an infinite-dimensional graded Th-module that satisfies all the properties listed Theorem 3.2. Then, for g an element of order 19 in Th, we can combine Proposition 3.1 and Proposition 5.1 to get the following expression for the coefficients of $\mathcal{F}_{19A}(\tau)$:

$$\operatorname{tr}(g|W_n) \equiv \frac{-4}{\sqrt{5}} \operatorname{Tr}_5^{(19)}(J^{(19,+)}; n) + (n_{19A} + \lambda_{19A} m_{19A}) b_{19A}(n), \tag{5.9}$$

where $b_{19A}(n)$ denotes the n^{th} coefficient of the weight $\frac{3}{2}$ cusp form $f_{19A} \in S_{19A}$. Since W is a virtual module for the Thompson group, we know the following congruence holds for each $p|\#Th$ (and in particular for $p = 19$) and for all $n > 0$

$$\dim(W_n) \equiv \operatorname{tr}(g_p|W_n) \pmod{p}, \tag{5.10}$$

where g_p denotes an element of order p. Plugging in the values of n_g and m_g from Table A.4, we get,

$$\dim(W_n) \equiv \frac{-4}{\sqrt{5}} \operatorname{Tr}_5^{(19)}(J^{(19,+)}; n) + 18b_{19A}(n) \pmod{19}. \tag{5.11}$$

Thus for $n = |d|$ where d is a fundamental discriminant that satisfies the properties of Theorem 1.1, we use Lemma 5.2 to get:

$$\dim(W_{|d|}) \equiv \operatorname{tr}(g_{19}|W_{|d|}) \equiv 18b_{19A}(|d|) \pmod{19}. \tag{5.12}$$

This shows that the congruence in the statement of our theorem holds if and only if $19|b_{19A}(|d|)$, or by Lemma 5.3, if and only if

$$\operatorname{ord}_{19}\left(\frac{L_{E^d}(1)}{\Omega(E^d)}\right) > \operatorname{ord}_{19}\left(\frac{L_{E^{d_0}}(1)}{\Omega(E^{d_0})}\right). \tag{5.13}$$

A quick `MAGMA` computation for $d_0 = -4$ shows that the right-hand side is 0. Thus, if $\dim(W_{|d|}) \not\equiv 0 \pmod{19}$, then $L_{E^d}(1) \not\equiv 0 \pmod{19}$, and in particular, $L_{E^d}(1) \neq 0$. By Kolyvagin's work [38], this means that $E^d(\mathbb{Q})$ is finite. This completes the proof of Theorem 1.1.

5.4. Theorem 1.3

We need to develop some more background before proving Theorem 1.3. For ℓ prime, we let $c_\ell(E)$ denote the Tamagawa number of E at ℓ, defined as the finite index

$$c_\ell = [E(\mathbb{Q}_\ell) : E^0(\mathbb{Q}_\ell)], \tag{5.14}$$

where $E^0(\mathbb{Q}_\ell)$ is the subgroup of points which have good reduction at ℓ. If E has good reduction at ℓ, then $E(\mathbb{Q}_\ell) = E^0(\mathbb{Q}_\ell)$ and $c_\ell = 1$. In particular for a general elliptic curve defined over $\mathbb{Q}$, we have that $c_\ell = 1$ for all but finitely many primes ℓ. The following result of C. Skinner (see also [52]) gives a local version of the Birch and Swinnerton-Dyer Conjecture for certain elliptic curves.

Theorem 5.4 *([51], Theorem C). Let $E/\mathbb{Q}$ be an elliptic curve and $p \geq 3$ a prime of good ordinary or multiplicative reduction. Assume that the $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representation $E[p]$ is*

irreducible and that there exists a prime $p' \neq p$ at which E has multiplicative reduction and $E[p]$ ramifies. If $L_E(1) \neq 0$, then we have that

$$\mathrm{ord}_p\left(\frac{L_E(1)}{\Omega_E}\right) = \mathrm{ord}_p\left(\#Ш(E)\prod_{\ell} c_\ell(E)\right). \tag{5.15}$$

If $L_E(1) = 0$, then we have $\mathrm{Sel}_p(E) \neq \{0\}$.

In order to use Theorem 5.4 in our proof of Theorem 1.3, we first show that each elliptic curve E of conductor 14 satisfies the hypotheses of Theorem 5.4 in the following lemma.

Lemma 5.5. *Let $d < 0$ be a fundamental discriminant for which $\left(\frac{d}{7}\right) = -1$ and $\left(\frac{d}{2}\right) = 1$; then for each elliptic curve E of conductor 14 the following are true:*

(a) The d^{th} quadratic twist of E has multiplicative reduction at $p \in \{2, 7\}$;
(b) The $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representation $E^d[7]$ is irreducible; and
(c) $E^d[7]$ ramifies at 2.

Proof. Let $E/\mathbb{Q}$ be an elliptic curve given by a minimal Weierstrass model

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5.16}$$

and define the discriminant of E by the equation

$$\Delta(E) := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \tag{5.17}$$

where $b_2 := a_1^2 + 4a_4$, $b_4 := 2a_4 + a_1a_3$, $b_6 := a_3^2 + 4a_6$ and $b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. Then E has multiplicative reduction at p if and only if p divides the discriminant of E but not the quantity $c_4(E) := (a_1^2 + 4a_4)^2 - 24(2a_4 + a_1a_3)$. For each elliptic curve of conductor 14, we have that $a_1 = a_3 = 1$, $a_2 = 0$ and $a_3 \in \{-2731, -171, -36, -11, -1, 4\}$ (see [57, Elliptic Curve 14.a]). Thus, for each elliptic curve E of conductor 14, E has multiplicative reduction at $p \in \{2, 7\}$. Since twisting by a fundamental discriminant d only changes $\Delta(E)$ and $c_4(E)$ up to a power of d, and d is coprime to 14, this proves part (a).

Part (b) follows from a lemma of Serre [48] which shows that the Galois representation $E^d[7]$ is surjective and hence irreducible. Finally, part (c) follows from part (b) and (the contrapositive of) Theorem 1.1 of [46]. □

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. Fix $W = W^\lambda$ to be an infinite-dimensional graded Th-module that satisfies all the properties listed Theorem 3.2. Let g denote an element of order

14 in Th. As before, we can combine Proposition 3.1 and Proposition 5.1 to get the following expression for the trace of g on W:

$$\operatorname{tr}(g|W_n) = \frac{-4}{\sqrt{5}} \operatorname{Tr}_5^{(14)}(J^{(14,+)}; n) + (n_{14A} + \lambda_{14A}^{(1)} m_{14A}) b_{14A}(n). \tag{5.18}$$

Here, $b_{14A}(n)$ denotes the n^{th} coefficient of the weight $\frac{3}{2}$ cusp form $f_{14A} \in S_{14A}$. By Lemma 5.2, we get that for $n = |d|$ where d is a fundamental discriminant that satisfies the properties of Theorem 1.3, the first term on the right-hand side of the above equation is 0. Plugging in values of $n_g^{(1)}$ and $m_g^{(1)}$ from Table A.4, we get the following congruence

$$\operatorname{tr}(g|W_{|d|}) = \left(42 + 56\lambda_{14A}^{(1)}\right) b_{14A}(|d|) \pmod{49}. \tag{5.19}$$

Suppose first that $\operatorname{tr}(g|W_{|d|}) \not\equiv 0 \pmod{49}$. Then, $b_{14A}(|d|) \not\equiv 0 \pmod{7}$. By Lemma 5.3, this means that

$$\operatorname{ord}_7\left(\frac{L_{E^d}(1)}{\Omega(E^d)}\right) = \operatorname{ord}_7\left(\frac{L_{E^{d_0}}(1)}{\Omega(E^{d_0})}\right). \tag{5.20}$$

As before we can use `MAGMA` to check that the right-hand side of the above equation is 0 for each E of conductor 14. Thus, if $\operatorname{tr}(g|W_{|d|}) \not\equiv 0 \pmod{49}$ then $\operatorname{ord}_7\left(\frac{L_{E^d}(1)}{\Omega(E^d)}\right) = 0$ and in particular, $L_{E^d}(1) \neq 0$. By Lemma 5.5 and Theorem 5.4, we have that

$$\operatorname{ord}_7\left(\#Ш(E^d) \prod_\ell c_\ell(E^d)\right) = 0. \tag{5.21}$$

Thus, $Ш(E^d)[7]$ is trivial. Furthermore, the Mordell–Weil group $E^d(\mathbb{Q})$ is finite [38].

We now consider the case that $\operatorname{tr}(g|W_{|d|}) \equiv 0 \pmod{49}$ and assume that $\operatorname{tr}(g|W_4) \not\equiv 43 \pmod{49}$. We can once again use Proposition 3.1 and Proposition 5.1 to write

$$\operatorname{tr}(g|W_4) = \frac{-4}{\sqrt{5}} \operatorname{Tr}_5^{(14)}(J^{(14,+)}; 4) + \left(42 + 56\lambda_{14A}^{(1)}\right) b_{14A}(4) = -6 + (42 + 56\lambda_{14A}^{(1)}). \tag{5.22}$$

Our assumption on $\operatorname{tr}(g|W_4)$ gives us the congruence $(42 + 56\lambda_{14A}^{(1)}) \not\equiv 0 \pmod{49}$ and hence by Equation (5.19) we get that $7 \mid b_{14A}(|d|)$. By Lemma 5.3 we get

$$\operatorname{ord}_7\left(\frac{L_{E^d}(1)}{\Omega(E^d)}\right) > 0. \tag{5.23}$$

First suppose that $L_{E^d}(1) = 0$, then $\operatorname{Sel}_p(E) \neq 0$ by Theorem 5.4. So we can reduce to the case where $L_{E^d}(1) \neq 0$. In that case, again by Theorem 5.4, we get,

$$\operatorname{ord}_7\left(\#Ш(E^d) \prod_\ell c_\ell(E^d)\right) > 0. \tag{5.24}$$

Thus the only thing left to check is that 7 does not divide any of the Tamagawa numbers $c_\ell(E^d)$ for any choice of E and d. By Theorem VII.6.1 in Silverman I [50], $c_\ell(E^d) \leq 4$ for most of these cases. The only other possibility is when E^d has split multiplicative reduction at ℓ, in which case, $c_\ell(E^d) = \mathrm{ord}_\ell(\Delta(E^d)) = \mathrm{ord}_\ell(|d|^6\Delta(E)))$. The conditions on d in the theorem imply that $|d|$ is square-free and coprime to $\Delta(E)$ for all E of conductor 14. Thus, if $7 \mid c_\ell(E^d)$, for some ℓ then ℓ lies in $\{2, 7\}$ and 7 divides $\mathrm{ord}_\ell(\Delta(E))$ which is independent of d. A quick check reveals that this is never the case for an elliptic curve of conductor 14. □

Appendix A. Tables

Table A.1
Multipliers for each rational conjugacy class.

$[g]$	1A	2A	3A	3B	3C	4A	4B	5A	6A	6B
v, h	0,1	0,1	1,3	0,1	2,3	0,1	1,2	0,1	1,3	2,3

$[g]$	6C	7A	8A	8B	9A	9B	9C	10A	12AB	12 C
v, h	0,1	0,1	1,2	1,4	0,1	0,1	1,3	0,1	1,3	0,1

$[g]$	12D	13A	14A	15AB	18A	18B	19A	20A	21A	24AB
v, h	1,6	0,1	0,1	1,3	0,1	2,3	0,1	1,2	1,3	1,6

$[g]$	24CD	27A	27BC	28A	30AB	31AB	36A	36BC	39AB
v, h	1,12	1,3	1,3	0,1	2,3	0,1	0,1	0,1	1,3

Table A.2
p-regular sections.

p	2	2	2	2	2	2	2	2	2	3
K_g	1A	3A	3B	3C	5A	7A	9A	9C	15AB	1A
α	15	6	3	4	3	3	4	3	3	10
$R_{p,g}$	1A,2A 4A,4B 8A,8B	3A 6B 12AB	3B,3C 12C 24CD	6C 6A 12D	5A 10A 20A	7A 14A 28A	9A,18A 36A, 36BC	9C 18B	15AB 30AB	1A,3A, 3B 3C, 9A, 9B 9C,27A,27BC

p	3	3	3	3	3	3	3	3	3	5	5
K_g	2A	4A	4B	5A	7A	8A	8B	10A	13A	1A	2A
α	4	3	1	1	1	1	1	1	1	3	1
$R_{p,g}$	2A,6A 6B, 6C 18A,18B	4A 12AB 12C	4B 12D	5A 15AB	7A 21A	8A 24AB	8B 24CD	10A 30AB	13A 39AB	1A 5A	2A 10A

p	5	5	5	7	7	7	7	13	13	19	31
K_g	3C	4B	6A	1A	2A	3A	4A	1A	3A	1A	1A
α	1	1	1	2	1	1	1	1	1	1	1
$R_{p,g}$	3C 15AB	4B 20A	6A 30AB	1A 7A	2A 14A	3A 21A	4A 28A	1A 13A	3A 39AB	1A 19A	1A 31AB

Table A.3
List of non-zero cusp forms in S_g for each rational conjugacy class $[g]$ of Th.

$f_{12D}(q) =$	$q^4 - 2q^8 + 2q^{20} - 2q^{40} - 2q^{52} + 4q^{56} - 2q^{68} + 4q^{88} - q^{100} - 6q^{116} + 2q^{136} + 4q^{148} + O(q^{150})$
$f_{14A}(q) =$	$q^4 - q^7 - q^8 + 2q^{15} - q^{16} + q^{28} + q^{32} - q^{36} - 2q^{39} + q^{56} - 2q^{60} + q^{63} + q^{64} - 2q^{71} + 3q^{72} + 2q^{79} - 2q^{84} - 2q^{88} + 2q^{95} - q^{100} - q^{112} + 2q^{119} + 2q^{120} - 4q^{127} - q^{128} - 4q^{135} + q^{144} + 4q^{148} + O(q^{151})$
$f_{18B}(q) =$	$q^4 + q^7 - q^{16} - q^{28} - 3q^{31} + q^{40} - 2q^{52} + q^{55} + q^{64} + 2q^{79} + q^{88} + 2q^{100} + 2q^{103} + q^{112} + 3q^{124} - q^{127} - 4q^{136} - 2q^{148} + O(q^{150})$
$f_{19A}(q) =$	$q^4 - q^7 - q^{11} + q^{19} + q^{20} - 2q^{24} + q^{28} + q^{35} - q^{36} + 2q^{39} - q^{43} - q^{44} + q^{47} - q^{55} + q^{63} - 2q^{64} - q^{68} + q^{76} - q^{95} + 3q^{99} + 2q^{100} - 2q^{111} + 2q^{112} - 2q^{115} - q^{119} + 2q^{120} - 2q^{123} + q^{131} - 3q^{139} + q^{140} + O(q^{151})$
$f^{(1)}_{20A}(q) =$	$q^4 - q^{20} - 2q^{24} - q^{36} + 2q^{40} + 2q^{56} + 2q^{84} - q^{100} - 2q^{120} - 4q^{136} + O(q^{151})$
$f^{(2)}_{20A}(q) =$	$q^7 - q^{15} - q^{23} + q^{47} + q^{63} - 2q^{87} + 2q^{95} + q^{103} - 3q^{127} - 2q^{143} + O(q^{151})$
$f^{(1)}_{21A}(q) =$	$q^4 - q^{11} - q^{16} + q^{23} - q^{28} - q^{32} + q^{35} + q^{44} + q^{56} + q^{64} + 2q^{67} - q^{71} - 2q^{79} - 2q^{91} - q^{92} + q^{100} - q^{107} + q^{112} - q^{116} - q^{119} + 2q^{127} - 2q^{148} + O(q^{150})$
$f^{(2)}_{21A}(q) =$	$q^7 + q^8 - q^{11} - 2q^{16} - q^{23} + q^{32} + 2q^{43} + q^{56} - q^{71} - 2q^{88} - 2q^{91} - 2q^{92} + 2q^{95} + 4q^{100} + q^{107} - 2q^{116} - 4q^{127} + q^{128} - 2q^{140} + O(q^{150})$
$f_{24AB}(q) =$	$q^4 - q^8 - q^{20} + 2q^{40} - 2q^{52} + 2q^{56} + q^{68} - 4q^{88} - q^{100} + 3q^{116} - 2q^{136} + 4q^{148} + O(q^{150})$
$f^{(1)}_{24CD}(q) =$	$q^4 - q^{100} + O(q^{150})$
$f^{(2)}_{24CD}(q) =$	$q^7 - 2q^{15} - q^{31} + 4q^{39} - 2q^{63} - 3q^{79} + 2q^{87} + q^{103} + q^{127} - 2q^{135} + O(q^{150})$
$f^{(3)}_{24CD}(q) =$	$q^{16} + q^{20} - 2q^{32} - q^{52} + q^{68} + 2q^{80} - 3q^{116} + 2q^{148} + O(q^{150})$
$f^{(1)}_{28A}(q) =$	$q^4 - q^8 - q^{16} + q^{28} + q^{32} - q^{36} + q^{56} - 2q^{60} + q^{64} + 3q^{72} - 2q^{84} - 2q^{88} - q^{100} - q^{112} + 2q^{120} - q^{128} + q^{144} + 4q^{148} + 2q^{156} - 2q^{168} - 4q^{184} + q^{196} - q^{200} + O(q^{201})$
$f^{(2)}_{28A}(q) =$	$q^7 - 2q^{15} + 2q^{39} - q^{63} + 2q^{71} - 2q^{79} - 2q^{95} - 2q^{119} + 4q^{127} + 4q^{135} + O(q^{151})$
$f^{(1)}_{30AB}(q) =$	$q^4 + 2q^{15} - q^{16} + 2q^{24} - 2q^{36} - 4q^{39} - q^{40} + 2q^{55} - 2q^{60} + q^{64} - 4q^{79} + 4q^{84} - 2q^{96} - q^{100} + 4q^{111} - 4q^{120} + 2q^{135} + 2q^{136} + 2q^{144} + O(q^{150})$
$f^{(2)}_{30AB}(q) =$	$q^7 + q^8 + q^{20} - q^{28} - q^{32} - q^{40} - 2q^{47} + q^{52} - q^{55} - 2q^{68} - q^{80} + q^{88} + 2q^{95} - q^{103} + q^{112} - q^{127} + q^{128} + 2q^{143} + q^{148} + O(q^{150})$
$f^{(3)}_{30AB}(q) =$	$q^{11} - q^{15} + q^{16} - q^{19} - q^{20} - q^{24} + q^{35} + q^{36} + 2q^{39} + q^{44} - q^{55} - q^{56} - 3q^{59} + q^{60} - q^{76} + 2q^{79} - q^{80} - 2q^{84} + q^{91} + q^{96} + 3q^{104} - 2q^{111} + 2q^{115} + 2q^{120} - q^{131} - q^{135} - 3q^{136} + q^{140} - q^{144} + O(q^{150})$
$f^{(1)}_{31AB}(q) =$	$q^4 - q^8 - q^{20} - q^{28} + q^{32} + 2q^{35} + q^{36} - 2q^{39} + q^{40} - 2q^{51} + q^{56} - 2q^{59} + 2q^{63} - q^{64} + 2q^{67} + 2q^{71} - q^{72} - q^{76} + 2q^{87} - 2q^{95} - 2q^{103} - 2q^{107} + q^{124} + 2q^{128} - 2q^{132} + q^{140} - 2q^{144} + O(q^{151})$
$f^{(2)}_{31AB}(q) =$	$q^7 - q^8 - q^{16} + q^{19} - q^{31} + q^{35} + 2q^{36} - q^{40} - 2q^{51} + q^{56} - q^{59} - q^{63} - q^{64} + q^{71} + q^{72} + 2q^{76} + q^{80} - q^{95} + q^{103} - q^{107} - 2q^{111} - q^{112} + q^{128} + q^{144} + O(q^{151})$
$f^{(1)}_{39AB}(q) =$	$q^7 - q^{19} + q^{20} - q^{31} - q^{32} - q^{44} - q^{59} + q^{67} + q^{71} + q^{80} + q^{83} + q^{91} + q^{104} - q^{119} - 2q^{124} + 2q^{136} - q^{143} + 2q^{148} + O(q^{150})$
$f^{(2)}_{39AB}(q) =$	$q^8 + q^{15} - q^{19} - q^{24} - q^{28} + q^{31} - q^{39} - q^{44} - q^{47} + q^{52} + q^{72} + q^{76} - q^{80} + q^{83} + 2q^{84} - q^{96} - q^{99} + q^{112} + 2q^{115} + q^{119} + q^{123} - q^{124} - q^{135} - q^{136} + O(q^{150})$
$f^{(3)}_{39AB}(q) =$	$q^{11} - q^{15} - q^{19} + q^{24} - q^{28} + q^{31} - q^{32} + q^{39} + q^{44} + q^{52} - q^{59} - q^{71} - q^{72} + q^{76} - q^{80} - 2q^{84} + q^{96} + q^{99} + q^{104} + q^{112} + 2q^{115} - q^{119} - q^{123} - q^{124} + q^{128} + q^{135} - q^{136} + q^{143} + O(q^{150})$

Table A.4
Integers $n_g^{(i)}$ and $m_g^{(i)}$ associated to each cusp form $f_g^{(i)}(\tau)$.

$f_g^{(i)}$	$n_g^{(i)}$	$m_g^{(i)}$	$f_g^{(i)}$	$n_g^{(i)}$	$m_g^{(i)}$	$f_g^{(i)}$	$n_g^{(i)}$	$m_g^{(i)}$	$f_g^{(i)}$	$n_g^{(i)}$	$m_g^{(i)}$
f_{12D}	12	24	f_{14A}	42	56	f_{18B}	0	18	f_{19A}	18	19
$f^{(1)}_{20A}$	0	20	$f^{(2)}_{20A}$	0	20	$f^{(1)}_{21A}$	9	21	$f^{(2)}_{21A}$	17	21
$f^{(1)}_{24AB}$	0	48	$f^{(1)}_{24CD}$	0	12	$f^{(2)}_{24CD}$	0	12	$f^{(3)}_{24CD}$	0	12
$f^{(1)}_{28A}$	0	14	$f^{(2)}_{28A}$	0	28	$f^{(1)}_{30AB}$	3	30	$f^{(2)}_{30AB}$	15	30
$f^{(3)}_{30AB}$	21	30	$f^{(1)}_{31A}$	2	31	$f^{(2)}_{31A}$	19	31	$f^{(1)}_{39AB}$	21	39
$f^{(2)}_{39AB}$	6	39	$f^{(3)}_{39AB}$	6	39						

References

[1] Amod Agashe, A visible factor of the special L-value, J. Reine Angew. Math. 2010 (644) (2010) 159–187.
[2] Arthur O.L. Atkin, Joseph Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. 185 (2) (1970) 134–160.
[3] Manjul Bhargava, Arul Shankar, Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0, Ann. Math. (2015) 587–621.
[4] Richard E. Borcherds, Monstrous moonshine and monstrous Lie superalgebras, Invent. Math. 109 (1) (1992) 405–444.
[5] Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system. I. The user language, in: Computational Algebra and Number Theory, London, 1993, J. Symb. Comput. (ISSN 0747-7171) 24 (3–4) (1997) 235–265, https://doi.org/10.1006/jsco.1996.0125.
[6] Christophe Breuil, Brian Conrad, Fred Diamond, Richard Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, J. Am. Math. Soc. 14 (4) (2001) 843–939.
[7] Kathrin Bringmann, Amanda Folsom, Ken Ono, Larry Rolen, Harmonic Maass Forms and Mock Modular Forms: Theory and Applications, vol. 64, American Mathematical Soc., 2017.
[8] Jan Hendrik Bruinier, Jens Funke, On two geometric theta lifts, Duke Math. J. 125 (1) (2004) 45–90.
[9] Scott Carnahan, Generalized moonshine IV: monstrous Lie algebras, arXiv preprint, arXiv:1208.6254, 2012.
[10] Miranda C.N. Cheng, John F.R. Duncan, On Rademacher sums, the largest Mathieu group and the holographic modularity of moonshine, Commun. Number Theory Phys. (ISSN 1931-4523) 6 (3) (2012) 697–758, https://doi.org/10.4310/CNTP.2012.v6.n3.a4.
[11] Miranda C.N. Cheng, John F.R. Duncan, Rademacher sums and Rademacher series, in: Conformal Field Theory, Automorphic Forms and Related Topics, Springer, 2014, pp. 143–182.
[12] Miranda C.N. Cheng, John F.R. Duncan, Jeffrey A. Harvey, Umbral moonshine, Commun. Number Theory Phys. (ISSN 1931-4523) 8 (2) (2014) 101–242, https://doi.org/10.4310/CNTP.2014.v8.n2.a1.
[13] Miranda C.N. Cheng, John F.R. Duncan, Jeffrey A. Harvey, Umbral moonshine and the Niemeier lattices, Res. Math. Sci. (ISSN 2522-0144) 1 (2014) 3, https://doi.org/10.1186/2197-9847-1-3.
[14] Miranda C.N. Cheng, John F.R. Duncan, Jeffrey A. Harvey, Weight one Jacobi forms and umbral moonshine, J. Phys. A (ISSN 1751-8113) 51 (10) (2018) 104002, https://doi.org/10.1088/1751-8121/aaa819.
[15] Henri Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, ISBN 3-540-55640-0, 1993.
[16] John H. Conway, Simon P. Norton, Monstrous moonshine, Bull. Lond. Math. Soc. 11 (3) (1979) 308–339.
[17] John H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups, Oxford University Press, Eynsham, ISBN 0-19-853199-0, 1985, with computational assistance from J.G. Thackray.
[18] Charles W. Curtis, Irving Reiner, Representation Theory of Finite Groups and Associative Algebras, Wiley Classics Library, John Wiley & Sons, Inc., New York, ISBN 0-471-60845-9, 1988, reprint of the 1962 original, a Wiley-Interscience Publication.
[19] Atish Dabholkar, Sameer Murthy, Don Zagier, Quantum black holes, wall crossing, and mock modular forms, arXiv preprint, arXiv:1208.4074, 2012.
[20] John F.R. Duncan, From the monster to Thompson to O'Nan, arXiv preprint, arXiv:1909.09684, 2019.
[21] John F.R. Duncan, Igor B. Frenkel, Rademacher sums, moonshine and gravity, Commun. Number Theory Phys. (ISSN 1931-4523) 5 (4) (2011) 849–976, https://doi.org/10.4310/CNTP.2011.v5.n4.a4.
[22] John F.R. Duncan, Michael J. Griffin, Ken Ono, Proof of the umbral moonshine conjecture, Res. Math. Sci. (ISSN 2522-0144) 2 (2015) 26, https://doi.org/10.1186/s40687-015-0044-7.
[23] John F.R. Duncan, Michael H. Mertens, Ken Ono, Pariah moonshine, Nat. Commun. 9 (1) (2017), https://doi.org/10.1038/s41467-017-00660-y.
[24] John F.R. Duncan, Michael H. Mertens, Ken Ono, O'Nan moonshine and arithmetic, arXiv preprint, arXiv:1702.03516, 2017.
[25] Walter Feit, The computations of some Schur indices, Isr. J. Math. (ISSN 0021-2172) 46 (4) (1983) 274–300, https://doi.org/10.1007/BF02762888.
[26] Paul Fong, Characters arising in the monster-modular connection, in: The Santa Cruz Conference on Finite Groups, Univ. California, Santa Cruz, Calif., 1979, in: Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., Providence, RI, 1980, pp. 557–559.

[27] David Ford, John McKay, Simon Norton, More on replicable functions, Commun. Algebra 22 (13) (1994) 5175–5193.
[28] Igor Frenkel, James Lepowsky, Arne Meurman, Vertex Operator Algebras and the Monster, Pure and Applied Mathematics, vol. 134, Academic Press, Inc., Boston, MA, ISBN 0-12-267065-5, 1988.
[29] Terry Gannon, Much ado about Mathieu, Adv. Math. 301 (2016) 322–358.
[30] GAP, GAP – Groups, Algorithms, and Programming, Version 4.10.1, The GAP Group, https://www.gap-system.org, 2019.
[31] Michael J. Griffin, Michael H. Mertens, A proof of the Thompson moonshine conjecture, Res. Math. Sci. 3 (1) (2016) 36.
[32] Benedict H. Gross, Don B. Zagier, Heegner points and derivatives of L-series, Invent. Math. (ISSN 0020-9910) 84 (2) (1986) 225–320, https://doi.org/10.1007/BF01388809.
[33] Jeffrey Harvey, Brandon Rayhaun, Traces of singular moduli and moonshine for the Thompson group, Commun. Number Theory Phys. 10 (2015), https://doi.org/10.4310/CNTP.2016.v10.n1.a2.
[34] Eric Hofmann, Liftings and Borcherds products, in: L-Functions and Automorphic Forms, in: Contrib. Math. Comput. Sci., vol. 10, Springer, Cham, 2017, pp. 333–366.
[35] Winfried Kohnen, Modular forms of half-integral weight on $\Gamma_0(4)$, Math. Ann. (ISSN 0025-5831) 248 (3) (1980) 249–266, https://doi.org/10.1007/BF01420529.
[36] Winfried Kohnen, Newforms of half-integral weight, J. Reine Angew. Math. (ISSN 0075-4102) 333 (1982) 32–72, https://doi.org/10.1515/crll.1982.333.32.
[37] Winfried Kohnen, Fourier coefficients of modular forms of half-integral weight, Math. Ann. 271 (2) (1985) 237–268.
[38] Victor A. Kolyvagin, Finiteness of and for a subclass of Weil curves, Math. USSR, Izv. 32 (3) (1989) 523.
[39] Alison Miller, Aaron Pixton, Arithmetic traces of non-holomorphic modular invariants, Int. J. Number Theory 6 (01) (2010) 69–87.
[40] J.S. Milne, Elliptic Curves, BookSurge Publishers, ISBN 1-4196-5257-5, 2006.
[41] S.P. Norton, Generalized moonshine, in: Proc. Symp. Pure Math., vol. 47, 1987, pp. 208–209.
[42] Ken Ono, The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series, CBMS Regional Conference Series in Mathematics, vol. 102, American Mathematical Society, Providence, RI, ISBN 0-8218-3368-5, 2004, published for the Conference Board of the Mathematical Sciences, Washington, DC.
[43] Ken Ono, Unearthing the visions of a master: harmonic Maass forms and number theory, Curr. Dev. Math. 2008 (2009) 347–454.
[44] PARI/GP version `2.11.2`, The PARI Group, Univ. Bordeaux, available from http://pari.math.u-bordeaux.fr/, 2019.
[45] Larissa Queen, Modular functions arising from some finite groups, Math. Comput. (ISSN 0025-5718) 37 (156) (1981) 547–580, https://doi.org/10.2307/2007446.
[46] Kenneth A. Ribet, On modular representations of arising from modular forms, Invent. Math. 100 (1) (1990) 431–476.
[47] Jeremy Rouse, John J. Webb, On spaces of modular forms spanned by eta-quotients, Adv. Math. 272 (2015) 200–224.
[48] Jean-Pierre Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (4) (1971) 259–331.
[49] J.-P. Serre, H.M. Stark, Modular forms of weight 1/2, in: Modular Functions of One Variable, VI, Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976, in: Lecture Notes in Math., vol. 627, 1977, pp. 27–67.
[50] Joseph H. Silverman, The Arithmetic of Elliptic Curves, vol. 106, Springer Science & Business Media, 2009.
[51] Christopher Skinner, Multiplicative reduction and the cyclotomic main conjecture for gl_2, Pac. J. Math. 283 (1) (2016) 171–200.
[52] Christopher Skinner, Eric Urban, The Iwasawa main conjectures for GL_2, Invent. Math. (ISSN 0020-9910) 195 (1) (2014) 1–277, https://doi.org/10.1007/s00222-013-0448-1.
[53] Stephen D. Smith, On the head characters of the Monster simple group, in: Finite Groups—Coming of Age, Montreal, Que., 1982, in: Contemp. Math., vol. 45, Amer. Math. Soc., Providence, RI, 1985, pp. 303–313.
[54] Jacob Sturm, On the congruence of modular forms, in: Number Theory, Springer, 1987, pp. 275–280.
[55] John T. Tate, The arithmetic of elliptic curves, Invent. Math. (ISSN 0020-9910) 23 (1974) 179–206, https://doi.org/10.1007/BF01389745.

[56] Richard Taylor, Andrew Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. Math. 141 (3) (1995) 553–572.
[57] The LMFDB Collaboration, The L-functions and modular forms database, http://www.lmfdb.org, 2013.
[58] John G. Thompson, Finite groups and modular functions, Bull. Lond. Math. Soc. (ISSN 0024-6093) 11 (3) (1979) 347–351, https://doi.org/10.1112/blms/11.3.347.
[59] John G. Thompson, Some numerology between the Fischer-Griess monster and the elliptic modular function, Bull. Lond. Math. Soc. 11 (3) (1979) 352–353.
[60] Masaru Ueda, The decomposition of the spaces of cusp forms of half-integral weight and trace formula of Hecke operators, J. Math. 11 (1988) 505–555.
[61] Masaru Ueda, Shunsuke Yamana, On newforms for Kohnen plus spaces, Math. Z. 264 (1) (2010) 1.
[62] Andrew Wiles, Modular elliptic curves and Fermat's last theorem, Ann. Math. 141 (3) (1995) 443–551.
[63] Andrew Wiles, The Birch and Swinnerton-Dyer conjecture, in: The Millennium Prize Problems, Clay Math. Inst., Cambridge, MA, 2006, pp. 31–41.
[64] Don Zagier, Traces of singular moduli, in: F. Bogomolov, L. Katzarkov (Eds.), Motives, Polylogarithms and Hodge Theory, in: Lecture Series, vol. 3, International Press, Somerville, 2002, pp. 209–244.