Max-Planck-Institut für Mathematik
Bonn

O'Nan moonshine and arithmetic

by

John F. R. Duncan
Michael H. Mertens
Ken Ono

Max-Planck-Institut für Mathematik
Preprint Series 2017 (12)

O'Nan moonshine and arithmetic

John F. R. Duncan
Michael H. Mertens
Ken Ono

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Department of Mathematics and
Computer Science
Emory University
400 Dowman Drive
Atlanta, GA 30322
USA

MPIM 17-12

O'NAN MOONSHINE AND ARITHMETIC

JOHN F. R. DUNCAN, MICHAEL H. MERTENS, AND KEN ONO

ABSTRACT. We prove the existence of a graded infinite-dimensional module for the sporadic simple group of O'Nan, for which the McKay–Thompson series are weight 3/2 mock modular forms. These series are linear combinations of generating functions for traces of singular moduli, class numbers, and central critical values of quadratic twists of weight 2 modular L-functions. As a consequence, for primes p dividing the order of the O'Nan group we obtain congruences between O'Nan group character values and class numbers, p-parts of Selmer groups, and Tate–Shafarevich groups of certain elliptic curves. This work represents the first example of moonshine involving arithmetic invariants of this type, and provides evidence supporting the view that moonshine is a phenomenon in which infinite-dimensional graded modules organize the arithmetic of products of Jacobians of modular curves.

1. Introduction and Statement of Results

The sporadic simple groups are the twenty-six exceptions to the classification [1] of finite simple groups: those examples that aren't included in any of the natural families. So by definition they are unnatural. Do they appear in nature?

At least for the *monster*, being the largest of the sporadics, the answer appears to be positive. By the last decade of the last century, Ogg's observation [59] on primes dividing the order of the monster, McKay's famous formula

$$196884 = 1 + 196883,$$

and the much broader family of coincidences observed by Thompson [71, 72] and Conway–Norton [24], were proven by Borcherds [6] to reflect the existence of a certain distinguished algebraic structure. This *moonshine module*, constructed by Frenkel–Lepowsky–Meurman [36, 37, 38], admits the monster as its full symmetry group, and has modular functions for traces. It is a cornerstone of *monstrous moonshine*, and indicates a pathway by which ideas from theoretical physics, and string theory in particular, may ultimately reveal a natural origin for the monster group and its curious connection to modularity.

In addition to the monster itself, nineteen of the sporadic simple groups appear as quotients of subgroups of the monster. As such, we may expect that monstrous moonshine extends to them in some form. This is consequent upon the *generalized moonshine conjecture*, which was formulated by Norton [58] following preliminary observations of Conway–Norton [24] and Queen [62], and has been recently proven in powerful work by Carnahan [17].

The theory of moonshine has deepened in this century. In 2010, Eguchi–Ooguri–Tachikawa [34] sparked a resurgence in the field with their observation that the elliptic genus of a K3 surface—a trace function arising from a non-linear sigma model with K3 target—is,

2010 *Mathematics Subject Classification.* 11F22, 11F37.

essentially, the product of an indefinite theta function and a q-series whose coefficients are dimensions of modules for Mathieu's largest sporadic group, M_{24}. In fact, this q-series is a mock modular form which, together with most of Ramanujan's mock theta functions, belongs to a family of distinguished examples [20] arising from a family of finite groups. This is *umbral moonshine* [21, 22, 23], and the existence of corresponding umbral moonshine modules has been verified by Gannon [40] in the case of M_{24}, and in general by Griffin and two of the authors of this work [32]. We refer the reader to [38, 39] for fuller discussions of monstrous moonshine, and to [33] for an updated account that includes umbral developments.

Very recently, yet another form of moonshine has appeared in work of Harvey–Rayhaun [48] which manifests a kind of half-integral weight enrichment of generalized moonshine for Thompson's sporadic group. The existence of a corresponding module has been confirmed by Griffin and one of the authors [44].

All the umbral groups are involved in the monster in some way, so we are left to wonder if there are natural explanations for the remaining six *pariah* sporadic groups: the *Janko groups* J_1, J_3, and J_4, the *Lyons group* Ly, the *Rudvalis group* Ru, and the *O'Nan group* $O'N$. Can moonshine shed light on these groups too?

Rudvalis group analogues of the moonshine module were constructed in [29, 30], but the physical significance of these structures is yet to be illuminated. In this work we present a new form of moonshine which reveals a role for the O'Nan group in arithmetic: as an organizing object for congruences between class numbers, p-parts of Selmer groups and Tate–Shafarevich groups of elliptic curves. This is the first occurrence of moonshine of this type. Since J_1 is a subgroup of $O'N$, it shows that at least two pariah groups play an active part in some of the deepest open questions in arithmetic.

1.1. **Moonshine and Divisors.** Before describing our results in more detail we offer a more conceptual perspective on moonshine. Suppose that G is a finite group. Loosely speaking, moonshine is a phenomenon which associates an infinite-dimensional graded G-module, say V^G, to a collection of modular forms, one for each conjugacy class. For monstrous, umbral, and Thompson moonshine we have

$$V^G = \bigoplus_m V_m^G \quad \xrightarrow{\textit{moonshine}} \quad (f_{[g]}) \in \begin{cases} \bigoplus_{[g]\in\mathrm{Conj}(G)} M_0^!(\Gamma_{[g]}) & \text{monstrous} \\ \\ \bigoplus_{[g]\in\mathrm{Conj}(G)} H_{\frac{1}{2}}(\Gamma_{[g]}) & \text{umbral, Thompson.} \end{cases}$$

The defining feature of the $f_{[g]}$ is that their m^{th} coefficients equal the graded traces $\mathrm{tr}(g|V_m^G)$.

In monstrous moonshine, the $f_{[g]}$ are Hauptmoduln for genus 0 groups $\Gamma_{[g]}$ (essentially level $o(g)$ congruence subgroups). At the cusp ∞, they have Fourier expansion

$$f_{[g]} = q^{-1} + O(q)$$

(note $q := e^{2\pi i\tau}$ throughout), and are holomorphic at other cusps. In particular, this means that $\mathrm{div}(f_{[g]}) = cz - \infty$ for some $z \in X(\Gamma_{[g]})$. In contrast, the $f_{[g]}$ in umbral and Thompson moonshine are not functions on modular curves, so it does not generally make sense to consider their divisors. Instead, they are weight $1/2$ harmonic Maass forms (with multiplier) for $\Gamma_{[g]}$, which means that the McKay–Thompson series are generally *mock modular forms*, the holomorphic parts of the $f_{[g]}$. Although they are not functions on these modular curves, it turns out that they actually encode even more information about divisors on $X(\Gamma_{[g]})$. For each discriminant D, there is a map Ψ_D for which

$$V^G = \bigoplus_m V_m^G \xrightarrow{\quad moonshine \quad} (f_{[g]}) \xrightarrow{\quad \Psi_D \quad} (\Psi_D(f_{[g]})) \in \bigoplus_{[g]\in \mathrm{Conj}(G)} \mathcal{K}(\Gamma_{[g]}),$$

where $\mathcal{K}(\Gamma_{[g]})$ is the field of modular functions for $\Gamma_{[g]}$. The $\Psi_D(f_{[g]})$ are *generalized Borcherds products* as defined by Bruinier and one of the authors [16]. They are meromorphic modular functions with a discriminant D Heegner divisor, and their fields of definition are dictated by the Fourier coefficients of the $f_{[g]}$.

As the preceding discussion illustrates, monstrous, umbral, and Thompson moonshine are (surprising) phenomena in which a single infinite-dimensional graded G-module organizes information about divisors on products of modular curves that are in one-to-one correspondence with the conjugacy classes of G. Moreover, the levels of these modular curves are (essentially) the orders of elements in these classes. In the case of monstrous moonshine, the divisors are simple: they are of the form $cz - \infty$. In umbral and Thompson moonshine, we obtain Heegner divisors on $X(\Gamma_{[g]})$.

The appearance of Heegner divisors recalls the seminal work of Zagier [79] on traces of singular moduli on $X_0(1)$. Loosely speaking, Zagier proved that the generating function for such traces in D-aspect can be weight $3/2$ weakly holomorphic modular forms. One of his motivations was to offer a classical perspective on special cases of Borcherds' work [7] on infinite product expansions of modular forms with Heegner divisor.

Although Zagier's paper has inspired too many papers to mention, we highlight an important note by Gross [45]. Gross observed that these types of theorems could be recast in terms of *generalized Jacobians* with cuspidal moduli. In particular, the generalized Jacobian of $X_0(1)$ with respect to the cuspidal divisor $2(\infty)$ is isomorphic to the additive group, and so the sum of the conjugates of Heegner points in the generalized Jacobian is equal to the trace of their modular invariants.

Here we adopt this perspective. We view traces of singular moduli as functionals on Heegner divisors, and we use the fact that their generating functions when summed over these divisors are weight $3/2$ weakly holomorphic modular forms. This phenomenon is an extension of the celebrated theorem of Gross–Kohnen–Zagier [46] which asserts that the generating function for Heegner divisors on $X_0(N)$ are weight $3/2$ cusp forms with values in the Jacobian of $X_0(N)$. This earlier theorem can be thought of as a result on central critical values of quadratic twists of weight 2 modular L-functions. Recently, Bruinier–Li [15] have developed Gross' note, and obtained a general framework in which weight $3/2$ mock modular forms and modular forms naturally arise as generating functions of trace functionals of Heegner divisors.

1.2. **Main Results.** In view of these developments, it is natural to seek weight $3/2$ moonshine. One can loosely think of this as the moonshine obtained by summing weight $1/2$ moonshine in D-aspect (e.g. umbral and Thompson moonshine), where the resulting McKay–Thompson series are generating functions for the arithmetic of these Heegner divisors.

Namely, we seek moonshine of the form

$$V^G = \bigoplus_m V_m^G \quad \xrightarrow{\textit{moonshine}} \quad (f_{[g]}) \in \bigoplus_{[g]\in \mathrm{Conj}(G)} H_{\frac{3}{2}}(\Gamma_{[g]}) \otimes \mathrm{Jac}(X(\Gamma_{[g]})),$$

where $\mathrm{Jac}(X(\Gamma_{[g]})$ denotes a suitable generalized Jacobian of $X(\Gamma_{[g]})$. In such moonshine, the $f_{[g]}$ will be generating functions for suitable functionals over Heegner divisors. They will be sums of generating functions for traces of singular moduli, class numbers, and square-roots of central L-values of quadratic twists of weight 2 modular forms.

Here we establish the first example of moonshine of this type, and it is pleasing that pariah sporadic groups appear. We prove moonshine for the O'Nan group $O'N$, a group discovered in 1976 as part of the flurry of activity related to the classification of finite simple groups [60] and shown not to be involved in the monster by Griess [43, Lemma 14.5]. It has order $\#O'N = 2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$, and it has 30 conjugacy classes. It contains the first Janko group J_1, also not involved in the monster [75], as a subgroup.

Theorem 1.1. *There is an infinite-dimensional (virtual) graded O'N-module*

$$W := \bigoplus_{0<m\equiv 0,3 \pmod 4} W_m$$

and weight 3/2 mock modular forms $\{F_{1A}, F_{2A}, \ldots, F_{31A}, F_{31B}\}$*, one for each conjugacy class, with the property that*

$$F_{[g]} = -q^4 + 2 + \sum_{0<m\equiv 0,3 \pmod 4} \mathrm{tr}(g|W_m)q^m.$$

Moreover, each $F_{[g]}$ *is on the group* $\Gamma_0(4\cdot o(g))$ *and satisfies the Kohnen plus space condition.*

The mock modular forms $F_{[g]}$ will be precisely characterized in Section 3. They will turn out to be sums of generating functions of traces of singular moduli for Hauptmoduln (cf. Section 5), class numbers, and square-roots of central critical L-values of quadratic twists of weight 2 modular forms (cf. Section 4.2.2). The Hauptmoduln which arise have levels which are in one-to-one correspondence with the orders of elements in $O'N$. Namely, the Hauptmoduln which arise are for the genus 0 modular curves

$$\{X_0(N):\ N = 1,\ldots,8,10,12,16\} \ \cup\ \{X_0^+(N):\ N = 11,14,15,19,20,28,31\}, \tag{1.1}$$

where $X_0^+(N)$ is the usual modular curve corresponding to the extension of $\Gamma_0(N)$ by the level N Atkin–Lehner involutions.

Remark. We note that W is a *virtual* module, which means that the multiplicities of irreducible representations of $O'N$ in W_m can be negative integers. However, the proof of Theorem 1.1 will show that all such multiplicities are positive for $m \notin \{7, 8, 12\}$

Remark. Using the description of the dimensions of the graded components W_m in terms of traces of singular moduli (cf. Appendix D), we find that

$$\dim W_{163} = \frac{1}{2}(\alpha^2 + \alpha - 393768),$$

where

$$\alpha = \left\lceil e^{\pi\sqrt{163}} \right\rceil = \lceil 262537412640768743.99999999999250072... \rceil$$

denotes the Ramanujan constant.

Remark. We have $F_{1A} = -q^{-4} + 2 + 26752q^3 + 143376q^4 + O(q^7)$. If we set $F_{1A}^{(j)}(\tau) := \sum_{m=j \bmod 2} (\dim W_m) q^m$ and $\vartheta^{(j)}(\tau) := \sum_{n=j \bmod 2} q^{n^2}$ then $F_{1A}^{(0)}\vartheta^{(0)} + F_{1A}^{(1)}\vartheta^{(1)}$ is the derivative of the J-function, up to a scalar factor and a rescaling of τ. This leads to the identity

$$196884 = 5 \cdot 1 + 2 \cdot 26752 + 58311 + 85064,$$

where the summands on the right are dimensions of irreducible representations of $O'N$.

Armed with Theorem 1.1 and the explicit identities expressing the $F_{[g]}$ in terms of singular moduli, class numbers and critical L-values, it is natural to ask whether the infinite-dimensional $O'N$-module W reveals deep arithmetic information about the modular curves they organize, which include the positive genus curves

$$\{X_0(11),\ X_0(14),\ X_0(15),\ X_0(19),\ X_0(20),\ X_0(28),\ X_0(31)\}$$

related to the $X_0^+(N)$ in (1.1). For example, are there interesting congruences modulo primes $p | \#O'N$ which relate the graded components W_m to classical objects in number theory and arithmetic geometry? This is indeed the case, and we now describe surprising congruences which relate graded dimensions and traces of W to class numbers and Selmer groups and Tate–Shafarevich groups of elliptic curves.

Remark. Suppose that p is prime and g_n (resp. g_{np}) are elements of $O'N$ with order n (resp. np). Then by Theorem 1.1, we have that $\mathrm{tr}(g_n|W_m) \equiv \mathrm{tr}(g_{np}|W_m) \pmod{p}$ for all m. In particular, if $o(g) = p$, then for all m we have

$$\dim W_m \equiv \mathrm{tr}(g|W_m) \pmod{p}.$$

The following theorem concerns congruences modulo small primes p and ideal class groups of imaginary quadratic fields. Here and in the following, we denote by $H(D)$ the Hurwitz class number of positive definite binary quadratic forms of discriminant $-D < 0$ (cf. Section 5).

Theorem 1.2. *Suppose that $-D < 0$ is a fundamental discriminant. Then the following are true:*

(1) If $-D < -8$ is even and $g_2 \in O'N$ has order 2, then

$$\dim W_D \equiv \mathrm{tr}(g_2|W_D) \equiv -24H(D) \equiv 0 \pmod{2^4}.$$

(2) If $p \in \{3, 5, 7\}$, $\left(\frac{-D}{p}\right) = -1$ and $g_p \in O'N$ has order p, then

$$\dim W_D \equiv \mathrm{tr}(g_p|W_D) \equiv \begin{cases} -24H(D) \pmod{3^2} & \text{if } p = 3, \\ -24H(D) \pmod{p} & \text{if } p = 5, 7. \end{cases}$$

Remark. Systematic congruences which assert for $\left(\frac{-D}{p}\right) = -1$ that

$$\dim W_D \equiv -24H(D) \pmod{p}$$

do not seem to hold for $p \geq 17$. However, this congruence holds for $p = 13$, a bonus because $13 \nmid \#O'N$.

Remark. As the proof of Theorem 1.2 will reveal, it holds true that if $-D < -8$ is an even fundamental discriminant, then $H(D)$ is even, and $\dim W_D \equiv 0 \pmod{2^4}$.

In view of Theorem 1.2, it is natural to consider the primes $p = 11, 19$ and 31 which also divide $\#O'N$. For these primes, a refinement of the congruences above is necessary. In particular, for the primes 11 and 19 we obtain congruences which relate $\dim W_D$ to Selmer groups and Tate–Shafarevich groups of elliptic curves (cf. [67, Chapter X]).

Let $E/\mathbb{Q}$ be an elliptic curve given by

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

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$. For fundamental discriminants Δ, let $E(\Delta)$ denote its Δ-quadratic twist, and let $\mathrm{rk}(E(\Delta))$ denote its Mordell–Weil rank over $\mathbb{Q}$. The $O'N$-module W encodes deep information about the Selmer and Tate–Shafarevich groups of the quadratic twists of elliptic curves with conductor 11, 14, 15, and 19. To make this precise, suppose that ℓ is an odd prime. Then for each curve $E(\Delta)$ we have the short exact sequence

$$1 \to E(\Delta)/\ell E(\Delta) \to \mathrm{Sel}(E(\Delta))[\ell] \to Ш(E(D))[\ell] \to 1,$$

where $\mathrm{Sel}(E(D))[\ell]$ is the ℓ-Selmer group of $E(\Delta)$, and $Ш(E(D))[\ell]$ denotes the elements of the Tate–Shafarevich group $Ш(E(\Delta))$ with order dividing ℓ.

For $p = 11$ and 19, we let $E_p/\mathbb{Q}$ be the $\Gamma_0(p)$-optimal elliptic curves given by the Weierstrass models

$$E_{11}: \quad y^2 + y = x^3 - x^2 - 10x - 20,$$
$$E_{19}: \quad y^2 + y = x^3 + x^2 - 9x - 15,$$

see [55, Elliptic Curve 11.a2, Elliptic Curve 19.a2]. We obtain the following congruence relating the graded dimension $\dim W_D$ to class numbers of Selmer groups and Tate–Shafarevich groups of such twists.

Theorem 1.3. *Assume the Birch and Swinnerton-Dyer Conjecture. If $p = 11$ or 19 and $-D < 0$ is a fundamental discriminant for which $\left(\frac{-D}{p}\right) = -1$, and $g_p \in O'N$ has order p, then the following are true.*

(1) We have that $\mathrm{Sel}(E_p(-D))[p] \neq \{0\}$ if and only if

$$\dim W_D \equiv \mathrm{tr}(g_p|W_D) \equiv -24H(D) \pmod{p}.$$

(2) Suppose that $L(E_p(-D), 1) \neq 0$. Then we have that $\mathrm{rk}(E(-D)) = 0$. Moreover, we have $p | \#Ш(E_p(-D))$ if and only if

$$\dim W_D \equiv \mathrm{tr}(g_p|W_D) \equiv -24H(D) \pmod{p}.$$

Remark. The claim about ranks in Theorem 1.3 (2) is unconditional thanks to the work of Kolyvagin [54].

Remark. By Goldfeld's famous conjecture on ranks of quadratic twists of elliptic curves [42], it turns out that the hypothesis in Theorem 1.3 (2) is expected to hold for 100% of the $-D$ for which $\left(\frac{-D}{p}\right) = -1$. Therefore, for almost all such $-D$, we should have a test for determining the presence of order p elements in these Tate–Shafarevich groups.

Remark. There is a more complicated congruence for the prime $p = 31$. For fundamental discriminants $-D < 0$ satisfying $\left(\frac{-D}{31}\right) = -1$, we have that $\dim W_D \equiv \mathrm{tr}(g_{31}|W_D) \pmod{31}$ are related to the central critical values of the $-D$ twists of the L-function for the genus 2 curve

$$C: \quad y^2 + (x^3 + x + 1)y = x^5 + x^4 + x^3 - x - 1$$

(cf. [55, Genus 2 Curve 961.a.961.3]). Its L-function arises from the two newforms in $S_2(\Gamma_0(31))$ which are Galois conjugates. Namely, if $\phi := \frac{1+\sqrt{5}}{2}$ then the two newforms are f^σ and

$$f(\tau) := \sum_{n=1}^{\infty} a(n)q^n = q + \phi q^2 - 2\phi q^3 + (\phi - 1)q^4 + q^5 - (2\phi + 2)q^6 + O(q^7),$$

where $\sigma(\sqrt{5}) = -\sqrt{5}$. If $p \nmid 31$ is prime, then the local L-factor $L_p(T)$ at p is

$$L_p(T) := (1 - a(p)T + pT^2)(1 - \sigma(a(p))T + T^2).$$

Remark. Apart from the claims about $\mathrm{tr}(g_{17}|W_D)$ (there are no elements of order 17 in $O'N$), Theorem 1.3 holds for $p = 17$ as well. Namely, the congruences hold for E_{17}, the optimal $\Gamma_0(17)$ elliptic curve over $\mathbb{Q}$ (cf. [55, Elliptic Curve 17.a3]) given by

$$E_{17}: \quad y^2 + xy + y = x^3 - x^2 - x - 14.$$

The two theorems on congruences above only pertain to the dimensions of the graded components of the $O'N$-module W. We now turn to congruences for graded traces for elements of order 2 and 3. To this end, we let E_{14} and E_{15} be the corresponding optimal elliptic curves over $\mathbb{Q}$ (cf. see [55, Elliptic Curve 14.a6, Elliptic Curve 15.a5]) given by

$$E_{14}: \quad y^2 + xy + y = x^3 + 4x - 6,$$
$$E_{15}: \quad y^2 + xy + y = x^3 + x^2 - 10x - 10.$$

Using work of Skinner–Urban [68, 69] related to the Iwasawa main conjectures for GL_2, we obtain the following unconditional result.

Theorem 1.4. *Assume the notation above, and suppose that $N \in \{14, 15\}$. If p is the unique prime ≥ 5 dividing N, then let $\delta_p := \frac{p-1}{2}$ and let $p' := N/p$. If $-D < 0$ is a fundamental discriminant for which $\left(\frac{-D}{p}\right) = -1$ and $\left(\frac{-D}{p'}\right) = 1$, then the following are true.*

(1) We have that $\mathrm{Sel}(E_N(-D))[p] \neq \{0\}$ if and only if

$$\mathrm{tr}(g_{p'}|W_D) \equiv \mathrm{tr}(g_N|W_D) \equiv \delta_p \cdot (H(D) - \delta_p H^{(p')}(D)) \pmod{p}.$$

(2) Suppose that $L(E_N(-D), 1) \neq 0$. Then we have that $\mathrm{rk}(E(-D)) = 0$. Moreover, we have $p|\#\text{Ш}(E_N(-D))$ if and only if

$$\mathrm{tr}(g_{p'}|W_D) \equiv \mathrm{tr}(g_N|W_D) \equiv \delta_p \cdot (H(D) - \delta_p H^{(p')}(D)) \pmod{p}.$$

Remark. We note that Theorem 1.4 does not apply for $p = 2$ (resp. $p = 3$) when $N = 14$ (resp. $N = 15$). In the case of $p = 2$ the work of Skinner–Urban does not apply. For $p = 3$ the connection between graded traces and central values of Hasse-Weil L-functions does not hold. Namely, a critical hypothesis due to Kohnen in terms of eigenvalues of Atkin–Lehner involutions fails (cf. Proposition 4.4).

Remark. In view of the new results presented here, it is natural to wonder where one should look for further moonshine. It seems likely that other sporadic groups will fall within the scope of weight $3/2$ moonshine. In another direction, one can ask about other half-integral weights. Also, it is natural to wonder if there are extensions of moonshine to Shimura curves and varieties. Are there infinite-dimensional G-modules which organize the arithmetic of their divisors?

1.3. **Methods.** To prove Theorem 1.1, we employ the theory of Rademacher sums, harmonic Maass forms, and standard facts about the representation theory of finite groups. Namely, we make use of the character table of $O'N$ (cf. Table A.1), and the Schur orthogonality relations for group characters. In Section 2, we first recall essential facts about harmonic Maass forms and Rademacher sums. In Section 3, we prove a theorem which explicitly constructs weight $3/2$ harmonic Maass forms, one for each conjugacy class of $O'N$. Furthermore, we establish that the corresponding mock modular forms have integer Fourier coefficients. To complete the proof, we apply the Schur orthogonality relations to these functions to construct weight $3/2$ mock modular forms whose coefficients encode the multiplicities of the irreducibles of the graded components of the alleged module W. The proof is complete once it is established that these multiplicities are integral. Since the obstruction to integrality is bounded by group theoretical considerations, the proof of integrality follows by confirming sufficiently many congruence relations among these forms. These calculations confirm that W is a virtual module. However, as mentioned earlier, it turns out that the multiplicities of each irreducible are non-negative in W_m once $m > 12$. This claim follows from an analytic argument which involves bounding sums of Kloosterman sums. These statements are proved in Section 4. In Section 5 we recall properties of singular moduli, and we interpret the mock modular forms number theoretically in terms of singular moduli and class numbers and cusp forms. We prove Theorems 1.2, 1.3 and 1.4 in Section 6. These proofs require the explicit formulas for the $F_{[g]}$, the results in Section 5, and the work of Skinner–Urban on the Birch and Swinnerton-Dyer Conjecture. We conclude the paper in Section 7 with numerical examples of some of these results.

Acknowledgements

The authors thank Michael Griffin, Dick Gross, Winfried Kohnen, Martin Raum, and Jeremy Rouse for helpful comments. The authors also thank Drew Sutherland for calculations which appear in the examples offered in this paper.

2. Rademacher Sums and Harmonic Maass Forms

Harmonic Maass forms are now a central topic in number theory. Their study originates from the work of Bruinier–Funke [13] on geometric theta lifts and Zwegers' seminal work

[81] on Ramanujan's mock theta functions. These realizations played a central role in the work of Bringmann and one of the authors on the Andrews–Dragonette Conjecture and Dyson's partition ranks [10, 12]. For an overview on the subject of harmonic Maass forms and its applications in number theory and various other fields of mathematics, including mathematical physics, we refer the reader to [9, 26, 61, 80].

Here, we briefly recall the essential facts about harmonic Maass forms that are required in this paper. Namely, we recall Rademacher sums, and we describe their projection to Kohnen's plus space.

2.1. **Rademacher Sums.** Here and throughout, we let $\tau = u + iv$, $u, v \in \mathbb{R}$ denote a variable in the upper half-plane $\mathfrak{H}$ and we use the shorthands $e(\alpha) := e^{2\pi i\alpha}$ and $q := e(\tau)$.

Definition 2.1. *We call a smooth function* $f : \mathfrak{H} \to \mathbb{C}$ *a harmonic Maass form of* weight $k \in \frac{1}{2}\mathbb{Z}$ *of* level N *if the following conditions are satisfied:*

(1) We have $f|_k\gamma(\tau) = f(\tau)$ *for all* $\gamma \in \Gamma_0(N)$ *and* $\tau \in \mathfrak{H}$*, where we define*

$$f|_k\gamma(\tau) := \begin{cases} (c\tau+d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right) & \text{if } k \in \mathbb{Z} \\ \left(\left(\frac{c}{d}\right)\varepsilon_d\right)^{2k} \left(\sqrt{c\tau+d}\right)^{-2k} f\left(\frac{a\tau+b}{c\tau+d}\right) & \text{if } k \in \frac{1}{2}+\mathbb{Z}. \end{cases}$$

with

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

and where we assume $4|N$ *if* $k \notin \mathbb{Z}$.

(2) The function f *is annihilated by the* weight k hyperbolic Laplacian,

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

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

We denote the space of harmonic Maass forms of weight k*, level* N *by* $H_k(\Gamma_0(N))$*.*

Remark. We note that condition (3) in the definition above differs from other definitions which occur commonly in the literature. For example, *harmonic Maass forms with principal parts* are those forms for which the $O(v^c)$ bound is replaced by $O(e^{-cv})$ for $c > 0$. Namely, the harmonic Maass forms we consider here are permitted to have 0^{th} Fourier coefficients which are essentially powers of v.

For the basic properties of these functions, we again refer to the literature mentioned above. We mention however the following lemmas.

Lemma 2.2. *Let* $f \in H_k(\Gamma_0(N))$ *be a harmonic Maass form of weight* $k \neq 1$*. Then there is a canonical splitting*

$$f(\tau) = f^+(\tau) + f^-(\tau), \tag{2.1}$$

where for some $m_0 \in \mathbb{Z}$ we have the Fourier expansions

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

and

$$f^-(\tau) := \overline{c_f^-(0)} \frac{(4\pi v)^{1-k}}{k-1} + \sum_{n=1}^{\infty} \overline{c_f^-(n)} n^{k-1} \Gamma(1-k; 4\pi n v) q^{-n},$$

where $\Gamma(\alpha; x)$ denotes the usual incomplete Gamma function.

The q-series f^+ in (2.1)) is called the *holomorphic part* of the harmonic Maass form f. The next lemma seems to have been missed by the literature.

Lemma 2.3. *A harmonic Maass form whose holomorphic part vanishes at all cusps is a (holomorphic) cusp form.*

Proof. This is a direct consequence of the properties of the Bruinier–Funke pairing (cf. Proposition 3.5 in [13]). ☐

A convenient way to construct harmonic Maass forms or *mock modular forms*, which are holomorphic parts of harmonic Maass forms, is through *Rademacher sums*. These were introduced by Rademacher in his work on coefficients of the J-function [63], and further developed in the context of moonshine mainly by Cheng, Frenkel and one of the authors [18, 19, 31].

Rademacher sums can be thought of as low weight analogues of Poincaré series. For a fixed level N and some $K > 0$, we define the set

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

For an integer μ, we can use this to formally define the Rademacher sum

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

If convergent, these sums define mock modular forms of the indicated level and weight. Convergence for these series however is in general a delicate matter when the weight k is between 0 and 2. We will be interested in these series when the weight is $k = \frac{3}{2}$ in which case it has been established in [18, Section 5] that they do converge (possibly using a certain regularization explained in loc. cit.) and define holomorphic functions on $\mathfrak{H}$.

By construction, Rademacher sums are 1-periodic and therefore have a Fourier expansion. It is given in terms of infinite sums of *Kloosterman sums*

$$K_k(m, n, c) := \sum_{d \pmod c}^{*} \left(\frac{c}{d}\right) \varepsilon_d^{2k} e\left(\frac{m\overline{d} + nd}{c}\right) \tag{2.2}$$

weighted by Bessel functions. Here we have that $k \in \frac{1}{2} + \mathbb{Z}$, c is divisible by 4, the * at the sum indicates that it runs over primitive residue classes modulo c, and $\overline{d}$ denotes the multiplicative inverse of d modulo c. Computing the Fourier expansion of a Rademacher sum is basically a standard computation, see for instance [19, Section 3.1] and [61, Section 8.3].

Theorem 2.4. *Assuming locally uniform convergence, then for $\mu \leq 0$ and $k \in \frac{1}{2} + \mathbb{N}$ and $4|N$, the Rademacher sum $R^{[\mu]}_{N,k}$ defines a mock modular form of weight k for $\Gamma_0(N)$ whose shadow is given by a constant multiple of the Rademacher sum $R^{[-\mu]}_{N,2-k}$. Its Fourier expansion is given by*

$$R^{[\mu]}_{N,k}(\tau) = q^\mu + \sum_{n=1}^{\infty} c^{[\mu]}_{N,k}(n) q^n,$$

where

$$c^{[\mu]}_{N,k}(n) = -2\pi i^k \left|\frac{n}{\mu}\right|^{\frac{k-1}{2}} \sum_{\substack{c>0 \\ c\equiv 0 \pmod N}} \frac{K_k(\mu,n,c)}{c} \cdot I_{k-1}\left(\frac{4\pi\sqrt{|\mu n|}}{c}\right) \tag{2.3}$$

for $\mu < 0$ and

$$c^{[0]}_{N,k}(n) = (-2\pi i)^k \frac{n^{k-1}}{\Gamma(k)} \sum_{\substack{c>0 \\ c\equiv 0 \pmod N}} \frac{K_k(0,n,c)}{c^k}. \tag{2.4}$$

The completion $\widehat{R^{[\mu]}_{N,k}}$ of $R^{[\mu]}_{N,k}$ to a harmonic Maass form has a pole of order μ at the cusp ∞ and vanishes at all other cusps.

Remark. One can also consider Rademacher sums of weights $\leq 1/2$, which are the main subject of [18] and play a crucial rule in both umbral and Thompson moonshine. The formulas look very similar in those cases, but since they are not needed, we omit them here.

2.2. **Kohnen's Plus Space.** In [53], Kohnen introduced the notion of the so-called plus space, a natural subspace of weight $k + \frac{1}{2}$ cusp forms for $\Gamma_0(4N)$ which is isomorphic via the Shimura correspondence to the space of weight $2k$ cusp forms of level N as a Hecke module, provided that N is odd and square-free. This space is easily characterized via Fourier expansions. Namely, it consists of all forms in $S_{k+\frac{1}{2}}(\Gamma_0(4N))$ (or, by extension, $M^!_{k+\frac{1}{2}}(\Gamma_0(4N))$ and also $H_{k+\frac{1}{2}}(\Gamma_0(4N))$) whose Fourier coefficients are supported on exponents n with $n \equiv 0, (-1)^k \pmod 4$. There is a natural projection operator

$$|\,\mathrm{pr} : S_{k+\frac{1}{2}}(\Gamma_0(4N)) \to S^+_{k+\frac{1}{2}}(\Gamma_0(4N))$$

for N odd given in terms of slash operators (see loc. cit.), which extends to spaces of weakly holomorphic modular forms and harmonic Maass forms. The action of this projection operator on principal parts of harmonic Maass forms is described in the following lemma (cf. Lemma 2.9 in [44]).

Lemma 2.5. *Let N be odd and let $f \in H_{k+\frac{1}{2}}(\Gamma_0(4N))$ for some $k \in \mathbb{N}_0$. Suppose that*

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

for some $m > 0$ with $-m \equiv 0, (-1)^k \pmod 4$, and suppose also 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 ∞ and has 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 the purpose of this paper, we are particularly interested in the Fourier expansion of weight 3/2 Rademacher sums projected to the plus space (see the following section). Convergence for these follows along the same lines as in [18, Section 5]. The following proposition gives their Fourier expansion explicitly.

Proposition 2.6. *Consider the Rademacher sum $R^{[\mu]}_{4N,\frac{3}{2}}$ for $\mu \leq 0$ such that $\mu \equiv 0,3 \pmod 4$ and N odd. Then we have that*

$$R^{[\mu],+}_{4N,\frac{3}{2}}(\tau) := \left(R^{[\mu]}_{4N,\frac{3}{2}}|\,\mathrm{pr}\right)(\tau) = q^\mu + \sum_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}} c^{[\mu],+}_{4N,\frac{3}{2}}(n)q^n,$$

where we have

$$c^{[\mu],+}_{4N,\frac{3}{2}}(n) = \kappa(\mu,n)\sum_{c=1}^{\infty}\left(1+\delta_{odd}(Nc)\right)K_{\frac{3}{2}}(\mu,n,4Nc)\cdot\mathcal{I}(\mu,n,Nc), \tag{2.5}$$

with

$$\kappa(\mu,n) := \begin{cases} 2\pi e\left(-\frac{3}{8}\right) & \textit{if } \mu = 0, \\ 2\pi e\left(-\frac{3}{8}\right)(n/|\mu|)^{\frac{1}{4}} & \textit{otherwise,} \end{cases} \tag{2.6}$$

$$\delta_{odd}(n) := \begin{cases} 1 & \textit{if } n \textit{ is odd,} \\ 0 & \textit{otherwise,} \end{cases} \tag{2.7}$$

and

$$\mathcal{I}(\mu,n,c) := \begin{cases} \dfrac{(2\pi n)^{\frac{1}{2}}}{c^{\frac{3}{2}}\Gamma(3/2)} & \textit{if } m = 0, \\[2ex] \dfrac{I_{\frac{1}{2}}\left(\frac{4\pi\sqrt{|\mu n|}}{c}\right)}{c} & \textit{otherwise.} \end{cases} \tag{2.8}$$

The following proposition shows that the vanishing of Kloosterman sums automatically forces certain even-level Rademacher sums to be in the plus space.

Proposition 2.7. *The Rademacher sum $R^{[\mu]}_{\frac{3}{2},4N}$ is automatically in the plus space if N is even and $\mu \equiv 0,3 \pmod 4$. Moreover, if $N,\mu \equiv 0 \pmod 4$, then the Fourier coefficients of $R^{[\mu]}_{\frac{3}{2},4N}$ are supported on exponents divisible by 4.*

Proof. We begin by noting that if c is divisible by 8, then the Kloosterman sum $K(m,n,c)$ in (2.2) vanishes unless $m-n \equiv 0,3 \pmod 4$. If c is divisible by 16, the same sum vanishes unless $m \equiv n \pmod 4$. Therefore, the claim follows from Theorem 2.4. $\square$

Remark. This is an easy restatement (and slight correction) of [44, Lemma 2.10].

Remark. We note that the formulas in Proposition 2.6 also hold for even N if one defines the projection operator pr for even levels as a suitable sieving operator, which one easily sees by a comparison to Theorem 2.4.

3. The Relevant Mock Modular Forms

Here we use the results from the previous section to construct the weight 3/2 harmonic Maass forms which we will later prove correspond to the McKay–Thompson series for the *O'N*-module W whose existence shall be proved later. Namely, the main result here is the following theorem.

Theorem 3.1. *Assuming the notation above, the following are true.*

(1) For every conjugacy class $[g]$ of O'N there is a unique mock modular form

$$F_{[g]}(\tau) = -q^{-4} + 2 + \sum_{n=1} a_{[g]}(n)q^n \tag{3.1}$$

of weight 3/2 for the group $\Gamma_0(4o(g))$ satisfying the following conditions:

(a) $F_{[g]}(\tau)$ lies in the Kohnen plus space, i.e., $a_{[g]}(n) = 0$ if $n \equiv 1, 2 \pmod 4$.

(b) $F_{[g]}(\tau)$ has a pole of order 4 at the cusp ∞, a pole of order $\frac{1}{4}$ at the cusp $\frac{1}{o(g)}$ if $o(g)$ is odd (as forced by the projection to the plus space, see Lemma 2.5), and vanishes at all other cusps.

(c) We have $a_{[g]}(3) = \chi_7(g)$, and $a_{[g]}(4) = \chi_1(g) + \chi_{12}(g) + \chi_{18}(g)$, and $a_{[g]}(7)$ as given in Tables B.1 to B.3, where χ_j, for $j = 1, ..., 30$, denotes the j^{th} irreducible character of O'N as given in Table A.1.

(2) The function $F_{[g]}(\tau)$ above has integer Fourier coefficients. Furthermore, if $o(g) \neq 16$, then it is a weakly holomorphic modular form.

Remark. One can also give a more intrinsic description of the conditions in part (c) above. The proof of the theorem will show that $F_{[g]}$ is already determined by conditions (a) and (b) in part (1), for the 19 conjugacy classes $[g]$ such that $o(g) \notin \{11, 14, 15, 19, 28, 31\}$. For the remaining conjugacy classes we remark that whenever a prime p divides $o(g)$, we need the congruence

$$a_{[g]}(n) \equiv a_{[g']}(n) \pmod p \tag{3.2}$$

where $o(g') = o(g)/p$ in order for these to be generalized characters for *O'N*. Whenever one can choose[1] the coefficient $a_{[g]}(n)$ for the function $F_{[g]}$, one picks the least integer in absolute value satisfying (3.2) for all primes $p \mid o(g)$.

Proof of Theorem 3.1. Let $g \in$ *O'N* be any element. Then the difference of Rademacher sums

$$\widetilde{F}_{[g]}(\tau) := -R^{[-4]}_{\frac{3}{2},4o(g)}(\tau) + 2R^{[0]}_{\frac{3}{2},4o(g)}(\tau)$$

[1]This turns out to be the case for $n = 3$ and $o(g) \in \{11, 15\}$, for $n = 4$ for $o(g) \in \{14, 19\}$ and for $n \in \{4, 7\}$ for $o(g) \in \{28, 31\}$.

of level $4o(g)$ is a mock modular form with the correct principal part at infinity and vanishes at all other cusps by Theorem 2.4. If $o(g)$ is even, then we know from Proposition 2.7 that this function is in the plus space. If on the other hand, $o(g)$ is odd, then we use the projection operator $|\,\mathrm{pr}$ to map it into the plus space, which by Lemma 2.5 introduces an additional pole of order $\frac{1}{4}$ at the cusp $\frac{1}{o(g)}$. This establishes the existence of a function satisfying properties (a) and (b) in Theorem 3.1 (1).

By Lemma 2.3, we see immediately that the above properties determine a mock modular form uniquely up to cusp forms. Unless $o(g) \in \{11, 14, 15, 19, 28, 31\}$, there are no cusp forms of weight 3/2 in the plus space, so one checks directly that in all those cases condition (c) is satisfied. In the remaining cases, condition (c) uniquely determines the contribution from cusp forms, because, as one can check using standard computer algebra systems[2], any weight 3/2 cusp form of one of the given levels in the plus space is uniquely determined by the coefficients of q^3, q^4, and q^7.

It remains to show that for $o(g) \neq 16$ the function $F_{[g]}$ is actually weakly holomorphic instead of just mock modular. First suppose that $o(g)$ is odd or $2||o(g)$. Then, because in those cases $o(g)$ is square-free, the shadow of $F_{[g]}(\tau)$ must be a multiple of

$$\vartheta(\tau) := \sum_{n\in\mathbb{Z}} q^{n^2},$$

which follows from the Serre-Stark basis theorem [66]. We compute the Bruinier–Funke pairings (see Proposition 3.5 in [13])

$$\{\widehat{R^{[-4],+}_{\frac{3}{2},4o(g)}}(\tau), \vartheta(\tau)\} = 2c \qquad \text{and} \qquad \{\widehat{R^{[0],+}_{\frac{3}{2},4o(g)}}(\tau), \vartheta(\tau)\} = c,$$

where c is some constant, which immediately shows that the shadow of the mock modular form $F_{[g]}(\tau) = -R^{[-4],+}_{\frac{3}{2},4o(g)}(\tau) + 2R^{[0],+}_{\frac{3}{2},4o(g)}(\tau)$ is 0, whence it is indeed a weakly holomorphic modular form.

If $o(g)$ is divisible by 4 or 8, but not 16, the space of possible shadows is *a priori* 2-dimensional, generated by $\vartheta(\tau)$ and $\vartheta(4\tau)$, but Proposition 2.7 and the fact that the shadow of a Rademacher sum is again a Rademacher sum show that the shadow's Fourier coefficients must be supported on exponents divisible by 4. So in fact, only multiples of $\vartheta(4\tau)$ can occur as shadows and the same computation as above shows the claim, observing that the only order left over is $o(g) = 16$. $\square$

4. Proof of Theorem 1.1

Here we prove that the mock modular forms given in Theorem 3.1 are McKay–Thompson series for the infinite-dimensional *O'N*-module W. We begin by stating a refined form of Theorem 1.1.

Theorem 4.1. *There is an infinite-dimensional graded virtual O'N-module*

$$W = \bigoplus_{\substack{m=3 \\ m\equiv 0,3 \pmod 4}}^{\infty} W_m$$

[2]The authors used Magma [8] for these computations

such that we have

$$\operatorname{tr}(g|W_m) = a_{[g]}(m),$$

for all m*. Moreover,* W_m *is an honest O'N-module for* $m \notin \{7, 8, 12\}$ *(see Tables B.1 to B.3).*

We break down the proof of this theorem into separate pieces. Using the Schur orthogonality relations on the irreducible represenations of *O'N*, we construct weight $3/2$ mock modular forms whose coefficients are the multiplicities of the irreducible components if and only if W exists. Therefore, the proof of Theorem 4.1 boils down to proving that these multiplicities are integral and non-negative for $m \notin \{7, 8, 12\}$. In Section 4.1 we establish integrality of these alleged multiplicities, and then in Section 4.2 we establish the claim on non-negativity.

4.1. **Integrality of Multiplicities.** For every prime $p \mid \#O'N$, we find linear congruences among the alleged McKay–Thompson series. Here, we prove these, but first we note that their truth implies the following systematic congruences.

Theorem 4.2. *Let* $g_j \in O'N$ *of order* d_j*,* $j = 1, 2$*, with* $d_2 = p^c \cdot d_1$ *for some prime number* p *and* $c \geq 1$*. Then we have the congruence*

$$F_{[g_1]} \equiv F_{[g_2]} \pmod{p}.$$

In Appendix C, we list these congruences, which sometimes hold with higher prime power moduli than stated in Theorem 4.2. Assuming their correctness for the moment, we can show integrality just as described in [44]. For the convenience of the reader, we recall the method briefly.

Let $\mathbf{C} \in \mathbb{Z}^{30\times\infty}$ denote the matrix formed by the coefficients of the functions $F_{[g]}(\tau)$ for each of the 30 conjugacy classes of *O'N* (in practice one uses of course a $30 \times B$ matrix for some large B). Further denote by $\mathbf{X} \in \overline{\mathbb{Q}}^{30\times 30}$ the matrix whose rows are indexed by irreducible characters and whose columns are indexed by conjugacy classes of *O'N*, with

$$\mathbf{X}_{\chi,[g]} := \frac{\overline{\chi(g)}}{\#C(g)},$$

where $C(g)$ denotes the centralizer of $g \in O'N$. By the first Schur orthogonality relation we see that the matrix

$$\mathbf{m} := \mathbf{X}\mathbf{C}$$

gives the multiplicities of each irreducible representation in the alleged virtual representation in Theorem 4.1. Since there are repetitions among the rows of $\mathbf{C}$, because the functions $F_{[g]}(\tau)$ depend only on the order of elements in $[g]$, it does not have full rank, but by just deleting the repetitions it does turn out to have full rank, which is 18. Let $\mathbf{N}^* \in \mathbb{Z}^{18\times 30}$ denote the matrix performing this operation and let $\mathbf{N} \in \mathbb{Z}^{30\times 18}$ be the matrix that undoes it, so that

$$\mathbf{m} = \mathbf{X}\mathbf{N}\mathbf{N}^*\mathbf{C}.$$

Now for each prime $p \mid \#O'N$, we can reduce the matrix $\mathbf{N}^*\mathbf{C}$ according to the aforementioned congruences as in [44] by left-multiplying by a matrix $\mathbf{M}_p \in \mathbb{Q}^{18\times 18}$, which is easily seen to have full rank. Hence we get

$$\mathbf{m} = (\mathbf{X}\mathbf{N}\mathbf{M}_p^{-1}) \cdot (\mathbf{M}_p\mathbf{N}^*\mathbf{C}).$$

The congruences in Appendix C ensure that the matrix $\mathbf{M}_p\mathbf{N}^*\mathbf{C} \in \mathbb{Q}^{18\times\infty}$ has all integer entries and one can check directly that the matrix $\mathbf{XNM}_p^{-1} \in \overline{\mathbb{Q}}^{30\times 18}$ has p-integral (rational) entries for every p. This shows that $\mathbf{m}$ has p-integral entries as well for each $p \mid \#O'N$, hence its entries must be integers, as claimed.

It remains to show the congruences. Since by Theorem 3.1, all functions $F_{[g]}(\tau)$ with $o(g) \neq 16$ are weakly holomorphic modular forms, we can prove all the congruences not involving F_{16ABCD} with standard techniques from the theory of modular forms. Probably the most uniform way would be to multiply each of the congruences by the unique cusp form g in $S^+_{\frac{25}{2}}(\Gamma_0(4))$ such that $g(\tau) = q^4 + O(q^5)$ (which has integral coefficients), thereby reducing the problem to congruences among holomorphic modular forms of weight 14, which can be checked in all cases using the Sturm bound [70], which is at most 225 in all cases.

In order to prove the remaining 4 congruences, we note that

$$F_{16ABCD}(\tau) - 8\mathscr{H}(4\tau) + 32\mathscr{H}(16\tau) \in M^{+,!}_{\frac{3}{2}}(\Gamma_0(64)) \tag{4.1}$$

is a weakly holomorphic modular form, where $\mathscr{H}(\tau) = \sum_{n=0}^{\infty} H(n)q^n$ denotes the generating function of the Hurwitz class numbers of binary quadratic forms (see Section 5 and [49, 76]). This can be seen as follows: For each level N there is an even weight k and a unique (up to normalization) holomorphic modular form $g_N(\tau)$, whose divisor is supported only at the cusp ∞ of the modular curve $X_0(N)$ (see Lemma 13 in [64]). Using this, it is straightforward to construct a weakly holomorphic modular form $f_{16}(\tau) = q^{-4} + O(1) \in M^{+,!}_{\frac{3}{2}}(\Gamma_0(64))$, which has a pole of order 4 at ∞ and vanishing principal part at all other cusps. Hence the difference $F_{16ABCD}(\tau) - f_{16}(\tau)$ is a mock modular form for $\Gamma_0(64)$ of weight 3/2 which is bounded at all cusps. The space of such forms is well-known to be generated by a basis of $M_{\frac{3}{2}}(\Gamma_0(64))$, as well as the functions $\mathscr{H}(\tau), \mathscr{H}(4\tau)$, and $\mathscr{H}(16\tau)$. Solving the resulting linear system implies the claim in (4.1).

We further remark that in each congruence involving $F_{16ABCD}(\tau)$, the factor in front of said function has 2-adic valuation $\ell - 3$, where the congruence is modulo 2^ℓ. It thus suffices to show that the function $4\mathscr{H}(4\tau) - 16\mathscr{H}(16\tau)$ (which has rational, but 2-integral coefficients) is congruent to a modular form modulo 2^2, since then, the Sturm bound argument from above can be used to prove the congruences in Appendix C (with the same bound as above). To be more precise, we claim that

$$4\mathscr{H}(4\tau) \equiv \vartheta(16\tau)^3 \equiv \vartheta(16\tau) \pmod 4, \tag{4.2}$$

where the second congruence is of course obvious. The Hurwitz class number $H(n)$ is not 2-integral if and only if $n = 4m^2$, since only then is there exactly one class of binary quadratic forms containing the form $m(x^2+y^2)$, which is counted with multiplicity $\frac{1}{2}$, so that $H(4m^2) \in \frac{1}{2} + \mathbb{Z}$. Therefore we have the congruence $4\mathscr{H}(\tau) \equiv \vartheta(4\tau) \pmod 4$, ergo (4.2).

4.2. **Positivity of Multiplicities.** Denote by $\mathrm{mult}_j(n)$ the multiplicity of the irreducible character χ_j of $O'N$ in the virtual module W_n as in Theorem 4.1, whose associated generalized character is given by the coefficients $a_\bullet(n)$, cf. Theorem 3.1. Then the Schur orthogonality relations and the triangle inequality tell us that

$$\begin{aligned}\mathrm{mult}_j(n) &= \sum_{[g]\subseteq O\text{'}N} \frac{1}{\#C(g)} a_{[g]}(n)\overline{\chi_j(g)} \\ &\geq \frac{|a_1(n)|}{\#O\text{'}N}\chi_j(1) - \sum_{[g]\neq 1A} \frac{|a_{[g]}(n)|}{\#C(g)}|\chi_j(g)|,\end{aligned} \tag{4.3}$$

where the summation runs through all conjugacy classes of $O\text{'}N$. Hence in order to show the eventual positivity of all $\mathrm{mult}_j(n)$, we want to establish explicit lower bounds on $a_1(n)$ and upper bounds on $a_{[g]}(n)$ for $g \neq 1$. Recall that

$$F_{[g]}(\tau) = -q^{-4} + 2 + \sum_{n=1}^{\infty} a_{[g]}(n)q^n = -R^{[-4]}_{\frac{3}{2},4o(g)}(\tau) + 2R^{[0]}_{\frac{3}{2},4o(g)}(\tau) + \text{cusp form}.$$

We bound each of the components individually, following the strategy already employed in [32, 40, 44], which we sketch briefly for the convenience of the reader. Note however that in the cited papers, only the coefficients of one Rademacher sum had to be considered, since the "corrections" there were known to come from weight $\frac{1}{2}$ modular forms, whose coefficients are bounded, while in our case, also the corrections can grow with n.

Since the computations necessary to bound the contribution coming from the Rademacher sum $R^{[-4]}_{\frac{3}{2},4o(g)}$, which is obviously going to be the dominant part, have been carried out in detail in [40, 44], we omit them here. The idea is to use the known formula for the coefficients of the Rademacher sum in terms of infinite sums of Kloosterman sums weighted by I-Bessel functions, see Section 2. One then splits this sum into three parts, a dominant part, an absolutely convergent remainder term and a value of a *Selberg–Kloosterman zeta function*, the first two of which may be bounded by elementary means, and for the third, one uses Proposition 4.1 in [44] (which we note is directly applicable to our situation).

4.2.1. *Bounding Coefficients of Rademacher Sums.* From Proposition 5.2 below, we see that the index 0 Rademacher sum can be explicitly given in terms of generating functions of generalized Hurwitz class numbers $H^{(N)}(n)$ (see Section 5 for the definition). While strong bounds for class numbers are known (see for instance Chapter 23 in [52] and the references therein), they are usually not explicit. For our purposes, crude bounds on class numbers suffice.

Proposition 4.3. *For every $N \in \mathbb{N}$, $-D \leq -5$ a negative discriminant and $\varepsilon > 0$ we have*

$$H^{(N)}(D) \leq [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] c_\varepsilon D^\varepsilon \cdot \frac{\sqrt{D}}{2\pi}\left(1 + \frac{1}{2}\log D\right),$$

where we can choose

$$c_\varepsilon = \prod_{p<e^{\frac{1}{2\varepsilon}}} (2\varepsilon p^{1/\log p - 2\varepsilon}\log p)^{-1}.$$

Proof. First we note that we trivially have the bound $H^{(N)}(D) \leq [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]H^{(1)}(D)$ by definition. Now suppose for the moment that D is a fundamental discriminant. Then

Dirichlet's class number formula gives

$$H(D) = \frac{\sqrt{D}}{2\pi} \cdot L\left(1, \left(\frac{-D}{\bullet}\right)\right).$$

Theorem 13.3 of Chapter 12 in [50] tells us that for $D \geq 5$ we have the upper bound

$$L\left(1, \left(\frac{-D}{\bullet}\right)\right) < 1 + \frac{1}{2}\log D.$$

By [77, pp. 73f.], Dirichlet's formula is also valid for non-fundamental discriminants if only primitive forms are counted, so that we get the bound

$$H(D) \leq \tau_\square(D)\frac{\sqrt{D}}{2\pi}\left(1 + \frac{1}{2}\log D\right),$$

where $\tau_\square(n)$ denotes the number of square divisors of n. Considering the prime factorisation of D, it is elementary to see that $\tau_\square(D) \leq c_\varepsilon D^\varepsilon$ for any $\varepsilon > 0$ and c_ε as claimed. $\square$

This result together with Proposition 5.2 gives a sufficient and explicit bound for the coefficients of the Rademacher sum $R^{[0]}_{\frac{3}{2},4o(g)}$. For the actual computations we choose $\varepsilon = \frac{1}{8}$, which yields $c_\varepsilon \approx 10.6766$.

4.2.2. *Bounding Coefficients of Cusp Forms.* For $g \in O'N$ with

$$o(g) \in \{11, 14, 15, 19, 28, 31\},$$

there are non-trivial cusp forms in $S^+_{\frac{3}{2}}(\Gamma_0(4 \cdot o(g)))$ contributing to our modular forms $F_{[g]}$, see Appendix D. According to the Ramanujan–Petersson conjecture, the coefficients of these cusp forms should grow like $O(n^{\frac{1}{4}+\varepsilon})$ (for n square-free), unconditional bounds (again for square-free n) have been obtained by Iwaniec [51] for weights $\geq 5/2$ and Duke [27] for weight $3/2$ (see also [28]). These bounds have one main disadvantage for our purposes, namely that the constants involved in them are not explicit or not computable. Here, we outline how to give completely explicit and computable, but very crude, estimates for the cusp form coefficients in question.

Let $P^{[m]}_{4N}$ denote the cuspidal Poincaré series of weight $3/2$ characterized by the *Petersson coefficient formula*,

$$\langle f, P^{[m]}_{4N}\rangle = \frac{b_f(m)}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4N)]\sqrt{4m}} \quad \forall\ f(\tau) = \sum_{n=1}^{\infty} b_f(n)q^n \in S^+_{\frac{3}{2}}(\Gamma_0(4N)), \tag{4.4}$$

where the Petersson inner product on $S^+_{\frac{3}{2}}(\Gamma_0(4N))$ is defined by the usual double integral

$$\langle f_1, f_2\rangle = \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4N)]}\int_{\Gamma_0(4N)\backslash\mathfrak{H}} f_1(\tau)\overline{f_2(\tau)}y^{\frac{3}{2}}\frac{dx\,dy}{y^2}.$$

The Fourier coefficients of these Poincaré series are given in terms of infinite sums of Kloosterman sums times J-Bessel functions (see Proposition 4 in [53]), and essentially the same computation used to bound the coefficients of the Rademacher sums $R^{[-4]}_{\frac{3}{2},4N}$ can be used here as well. It is then only necessary to express the cusp forms $\mathscr{G}^{(o(g))}$ (see again

Appendix D) in terms of these Poincaré series, which is particularly easy in the cases where $o(g) \neq 31$ is odd, since in those cases, the space $S^+_{\frac{3}{2}}(\Gamma_0(4\cdot o(g)))$ is one-dimensional and $\mathscr{G}^{(o(g))}$ is a newform. Hence we have $\langle \mathscr{G}^{(o(g))}, P^{[m]}_{4N}\rangle = \beta\langle \mathscr{G}^{(o(g))}, \mathscr{G}^{(o(g))}\rangle$, where we choose m to be the order of $\mathscr{G}^{(o(g))}$ at ∞. It therefore remains to compute the Petersson norm of the newform $\mathscr{G}^{(o(g))}$. This can be done by means of the following result due to Kohnen, which is an explicit version of Waldspurger's theorem (see Corollary 1 in [53]).

Proposition 4.4. *Let $N \in \mathbb{N}$ be odd and square-free, $f \in S^+_{k+\frac{1}{2}}(\Gamma_0(4N))$ be a newform and $F \in S_{2k}(\Gamma_0(N))$ the image of f under the Shimura correspondence. For a prime $\ell | N$, set w_ℓ the eigenvalue of F under the Atkin–Lehner involution W_ℓ and choose a fundamental discriminant D with $(-1)^k D > 0$ and $\left(\frac{D}{\ell}\right) = w_\ell$ for all ℓ. Then we have*

$$\langle f, f\rangle = \frac{\langle F, F\rangle \pi^k}{2^{\omega(N)}(k-1)!|D|^{k-\frac{1}{2}}L(F, D; k)} \cdot |b_f(|D|)|^2,$$

where $L(F, D; s)$ denotes the twist of the newform F by the quadratic character $\left(\frac{D}{\bullet}\right)$ and $\omega(N)$ denotes the number of distinct prime divisors of N.

Since the twisted L-series has a functional equation of the usual type, there are efficient methods to compute its values numerically (the authors used the built-in intrinsics of Magma [8]). Computing the Petersson norm of F is also possible to high accuracy, e.g. by using the well-known relationship (cf. [25, 78])

$$\langle F, F\rangle = \frac{\mathrm{vol}(E)}{4\pi^2}\deg(\varphi_E),$$

if F is the newform is associated to the elliptic $E/\mathbb{Q}$, the covolume of whose period lattice we denote by $\mathrm{vol}(E)$ and whose modular parametrization[3] is given by φ_E, or for N prime using Theorem 2 in [78].

Remark. Kohnen's result Proposition 4.4 has been extended to many situations, e.g. by Ueda and his collaborators [73, 74] to certain even levels and forms not in the plus-space, see in particular Corollary 1 in [56], so that the above reasoning carries over to $o(g) \in \{14, 28\}$, by noting that $\mathscr{G}^{(14)}$ and $\mathscr{G}^{(28)}$ both arise from the unique normalized cusp form in $S_{\frac{3}{2}}(\Gamma_0(28))$ (not in the plus space), the former by applying sieve operators, the latter by applying the V_4-operator.

Remark. For $o(g) = 31$, the above reasoning only needs to be modified to take into account that $\mathscr{G}^{(31)}$ is not a Hecke eigenform, but its decomposition into newforms is given in Appendix D. Using that these newforms are orthogonal, the only difference becomes that one needs to take into account two Poincaré series instead of just one.

Putting the estimates for the Rademacher sums $R^{[-4]}_{\frac{3}{2},4o(g)}$, $R^{[0]}_{\frac{3}{2},4o(g)}$, as well as the occuring cusp forms together and plugging them all into (4.3), one finds that the multiplicities are

[3] Every elliptic curve E we consider in this paper has $\deg(\varphi_E) = 1$.

nonnegative as soon as $n \geq 109$ (the worst case occurs for the characters χ_1 and χ_2). Inspecting the remaining coefficients by computer then completes the proof of Theorem 4.1.

5. Traces of Singular Moduli

In this section, we discuss and recall some basic notation and facts about traces of singular moduli. Their study originates in seminal work by Zagier [79], and has since been an important subject in number theory (cf. for instance [4, 11, 14, 57], just to name a few). In the explicit context of moonshine for the Thompson group, traces of singular moduli of these functions appeared e.g. in [48].

5.1. **Genus Zero Orders.** It is well-known that for an element $g \in O'N$ with $o(g) \notin \{11, 14, 15, 19, 20, 28, 31\}$, the modular curve $X_0(o(g))$ has genus 0, so that in those cases, there is a Hauptmodul $J^{(o(g))}$, which can be given in terms of the Dedekind eta-function (cf. Table 5.1), which is given by

$$\eta(\tau) := q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n).$$

$o(g)$	1	2	3	4	5	6
$J^{(o(g))}(\tau)$	$\frac{E_4(\tau)^3}{\Delta(\tau)} - 744$	$\frac{\eta(\tau)^{24}}{\eta(2\tau)^{24}} + 24$	$\frac{\eta(\tau)^{12}}{\eta(3\tau)^{12}} + 12$	$\frac{\eta(\tau)^{8}}{\eta(4\tau)^{8}} + 8$	$\frac{\eta(\tau)^{6}}{\eta(5\tau)^{6}} + 6$	$\frac{\eta(\tau)^5\eta(3\tau)}{\eta(2\tau)\eta(6\tau)^5} + 5$

$o(g)$	7	8	10	12	16
$J^{(o(g))}(\tau)$	$\frac{\eta(\tau)^4}{\eta(7\tau)^4} + 4$	$\frac{\eta(\tau)^4\eta(4\tau)^2}{\eta(2\tau)^2\eta(8\tau)^4} + 4$	$\frac{\eta(\tau)^3\eta(5\tau)}{\eta(2\tau)\eta(10\tau)^3} + 3$	$\frac{\eta(\tau)^3\eta(4\tau)\eta(6\tau)^2}{\eta(2\tau)^2\eta(3\tau)\eta(12\tau)^3} + 3$	$\frac{\eta(\tau)^2\eta(8\tau)}{\eta(2\tau)\eta(16\tau)^2} + 2$

Table 5.1. Hauptmoduln for $\Gamma_0(o(g))$

Let us introduce some notation. Denote by $\mathcal{Q}_{-D}^{(N)}$ the set of positive definite quadratic forms $Q = ax^2 + bxy + cy^2 =: [a, b, c]$ of discriminant $-D = b^2 - 4ac < 0$ such that $N|a$. It is well-known that $\Gamma_0(N)$ acts on $\mathcal{Q}_{-D}^{(N)}$ with finitely many orbits, which correspond to the so-called *Heegner points* on the modular curve $X_0(N)$. 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 $\mathfrak{H}$. For a function $f : \mathfrak{H} \to \mathbb{C}$ invariant under the action of $\Gamma_0(N)$ we then define the trace function

$$\mathrm{Tr}_D^{(N)}(f) := \sum_{Q \in \mathcal{Q}_{-D}^{(N)}/\Gamma_0(N)} \frac{f(\tau_Q)}{\omega^{(N)}(Q)}, \tag{5.1}$$

where $\omega^{(N)}(Q) = \frac{1}{2} \cdot \#\,\mathrm{Stab}_{\Gamma_0(N)}(Q)$. Further let

$$\mathscr{H}^{(N)}(\tau) := -\frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]}{12} + \sum_{\substack{D>0 \\ D \equiv 0,3 \pmod 4}} H^{(N)}(D) q^D$$

denote the generating function of the *(generalized) Hurwitz class numbers of level N* which are defined as $H^{(N)}(D) := \mathrm{Tr}_D^{(N)}(1)$. The special case of $N = 1$ yields the classical Hurwitz class numbers $H^{(1)}(D) := H(D)$.

It is a straightforward consequence of Theorem 1.2 in [57], analogous to Theorem 1.2 in [4], that we can describe the Fourier coefficients of the Rademacher sums $R^{[-4],+}_{\frac{3}{2},4o(g)}$ as traces of the Hauptmoduln in Table 5.1.

Proposition 5.1. *Let $N \in \mathbb{N}$ such that $X_0(N)$ has genus 0 and*

$$\mathrm{Tr}_4^{(N)}(D) := \frac{1}{2}\left(\mathrm{Tr}_D^{(N)}(J_2^{(N)}) - \mathrm{Tr}_D^{(N/d)}(J^{(N/d)})\right), \tag{5.2}$$

where $J_2^{(N)} = q^{-2} + O(q)$ is the unique modular function for $\Gamma_0(N)$ with this Fourier expansion at infinity and no poles anywhere else and $d := \gcd(N, 2)$. Then we have

$$\mathscr{T}^{(N)}(\tau) := -q^{-4} + \sum_{\substack{D>0 \\ D\equiv 0,3 \pmod 4}} \mathrm{Tr}_4^{(N)}(D)q^D = R^{[-4],+}_{\frac{3}{2},4o(g)}(\tau) - \frac{c_2}{2}\mathscr{H}^{(N)}(\tau) + \frac{c_1}{2}\mathscr{H}^{(N/d)}(\tau) \tag{5.3}$$

for some rational numbers c_1 and c_2. In particular, the function $\mathscr{T}^{(N)}$ has integer Fourier coefficients.

Remark. It should be pointed out that Theorem 1.2 in [57] is only stated for odd levels, although the proof goes through for even levels as well.

Remark. The rational numbers c_j, $j = 1, 2$ in Proposition 5.1 are the constant terms of the weight 0 Rademacher sums $R^{[-2]}_{0,N}$ resp. $R^{[-1]}_{0,N/d}$. For a proof of the rationality of these numbers, see Lemma 3.2 in [4].

For the Rademacher sum $R^{[0],+}_{\frac{3}{2},4\cdot o(g)}$, we get the following.

Proposition 5.2. *For $N \in \mathbb{N}$, let $R := R^{[0],+}_{\frac{3}{2},4N}$ denote the Rademacher sum of weight $3/2$ of level N and index 0. Then we have*

$$R = -\frac{12}{\varphi(N)}\sum_{d|N}\frac{d}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(d)]}\mu\left(\frac{N}{d}\right)\mathscr{H}^{(d)},$$

where μ and φ denote the Möbius function and Euler's totient function respectively.

Proof. This follows from a straightforward modification of the proof of Theorem 1.2 in [57]. □

Note that the above proposition is indeed valid for all N, not just those where $X_0(N)$ has genus 0.

Putting Propositions 5.1 and 5.2 together, we obtain explicit descriptions of the functions $F_{[g]}$ in terms of singular moduli which are given in Appendix D.

5.2. **Positive Genus Orders.** In the remaining cases, i.e. where

$$o(g) \in \{11, 14, 15, 19, 20, 28, 31\},$$

the modular curve $X_0(o(g))$ has genus 2 for $o(g) \in \{28, 31\}$ and 1 otherwise, so there is no notion of a Hauptmodul there. However, it is known that for all these levels, the modular curve $X_0^+(o(g))$, the quotient of $X_0(o(g))$ by Atkin–Lehner involutions, has genus 0 (see e.g. [35]), so there exists a Hauptmodul $J^{(o(g),+)}(\tau)$ for the group $\Gamma_0^+(o(g))$, see Table 5.2. There, $f_{E_{19}}$ denotes the weight 2 newform associated to the elliptic curve

$$E_{19} : y^2 + y = x^3 + x^2 - 9x - 15$$

([55, Elliptic Curve 19.a2]) and $f_{31} = q + \frac{1+\sqrt{5}}{2}q^2 + O(q^3)$ denotes the unique newform in $S_2(\Gamma_0(31))$ up to Galois conjugation (which is denoted by an exponent σ).

$o(g)$	11	14
$J^{(o(g),+)}(\tau)$	$-\frac{E_2(\tau)-11E_2(11\tau)}{10\eta(\tau)^2\eta(11\tau)^2} - \frac{22}{5}$	$-\frac{E_2(\tau)+2E_2(2\tau)-7E_2(7\tau)-14E_2(14\tau)}{18\eta(\tau)\eta(2\tau)\eta(7\tau)\eta(14\tau)} - \frac{7}{3}$

$o(g)$	15	19
$J^{(o(g),+)}(\tau)$	$-\frac{E_2(\tau)+3E_2(3\tau)-5E_2(5\tau)-15E_2(15\tau)}{16\eta(\tau)\eta(3\tau)\eta(5\tau)\eta(15\tau)} - \frac{5}{2}$	$-\frac{E_2(\tau)-19E_2(19\tau)}{18f_{E_{19}}(\tau)} - \frac{4}{3}$

$o(g)$	20	28	31
$J^{(o(g),+)}(\tau)$	$\frac{\eta(2\tau)^8\eta(10\tau)^8}{\eta(\tau)^4\eta(4\tau)^4\eta(5\tau)^4\eta(20\tau)^4} - 4$	$\frac{\eta(2\tau)^6\eta(14\tau)^6}{\eta(\tau)^3\eta(4\tau)^3\eta(7\tau)^3\eta(28\tau)^3} - 3$	$\frac{\sqrt{5}(f_{31}(\tau)+f_{31}^\sigma(\tau))}{2(f_{31}(\tau)-f_{31}^\sigma(\tau))} - \frac{5}{2}$

TABLE 5.2. Hauptmoduln for $\Gamma_0^+(o(g))$

We can now again express the Fourier coefficients of the Rademacher sum $R^{[-4],+}_{\frac{3}{2},4o(g)}$ in terms of singular moduli of holomorphic modular functions and class numbers.

Proposition 5.3. *Let $N \in \mathbb{N}$ such that $X_0^+(N)$ has genus 0 and*

$$\operatorname{Tr}_4^{(N,+)}(D) := \frac{1}{2}\left(\frac{1}{2^{\omega(N)}}\operatorname{Tr}_D^{(N)}\left(J_2^{(N,+)}\right) - \frac{1}{2^{\omega(N/d)}}\operatorname{Tr}_D^{(N/d)}\left(J^{(N/d,+)}\right)\right), \tag{5.4}$$

where $J_2^{(N,+)} = q^{-2} + O(q)$ is the unique modular function for $\Gamma_0(N)^+$ with this Fourier expansion at infinity and no poles anywhere else and $d := \gcd(N,2)$. Then we have

$$\mathscr{T}^{(N,+)}(\tau) := q^{-4} + \sum_{\substack{D>0 \\ D\equiv 0,3 \pmod 4}} \operatorname{Tr}_4^{(N,+)}(D)q^D = R^{[-4],+}_{\frac{3}{2},4o(g)}(\tau) - \frac{c_2}{2}\mathscr{H}^{(N)}(\tau) + \frac{c_1}{2}\mathscr{H}^{(N/d)}(\tau) \tag{5.5}$$

for some rational numbers c_1 and c_2, where $\omega(N)$ denotes the number of distinct prime factors of N. Moreover, we have that $\mathscr{T}^{(N,+)}(\tau) \in \alpha_N \cdot q^{-4}\mathbb{Z}[[q]]$, where

$$\alpha_N := \begin{cases} 1 & \text{if } N \in \{11, 15, 19, 31\}, \\ \frac{1}{6} & \text{if } N = 14, \\ \frac{1}{4} & \text{if } N = 28. \end{cases}$$

Proof. Proposition 5.1 turns out to be valid for all N, if one replaces the Hauptmodul $J^{(N)}$ by the completed Rademacher sum $\widehat{R^{[-1]}_{0,N}}$, normalized so that its constant term is 0 and $J_2^{(N)}$ by $\widehat{R^{[-2]}_{0,N}}$ with the same normalization, which is the original formulation in [57]. Note that these Rademacher sums coincide with the Hauptmoduln where applicable. Now we consider for $N'||N$, i.e. $\gcd(N', N/N') = 1$, the Atkin–Lehner involution $W_{N'}$. These involutions map the set $\mathcal{Q}^{(N)}_{-D}/\Gamma_0(N)$ bijectively to itself (see e.g. Section 1 of [46]), so that we have for any $\Gamma_0(N)$-invariant function f that

$$\mathrm{Tr}^{(N)}_D(f) = \mathrm{Tr}^{(N)}_D(f|W_{N'}),$$

or alternatively, since there are exactly $2^{\omega(N)}$ Atkin–Lehner involutions of level N, that

$$\mathrm{Tr}^{(N)}_D(f) = \frac{1}{2^{\omega(N)}} \mathrm{Tr}^{(N)}_D(\sum_{N'||N} f|W_{N'}).$$

The function $\sum_{N'||N} f|W_{N'}$ is then clearly $\Gamma_0(N)^+$-invariant, hence in the case where $f = \widehat{R^{[-1]}_{0,N}}$ or $\widehat{R^{[-2]}_{0,N}}$ has to coincide with $J^{(N,+)}$ resp. $J_2^{(N,+)}$ up to a rational, additive constant, which proves the result. □

Again, the explicit expressions are given in Appendix D.

6. Number Theoretic Applications

In this section, we will prove the arithmetic applications of O'Nan moonshine given in Theorems 1.2 to 1.4. All these proofs rely on the following easy observation.

Lemma 6.1. *Let $N > 1$ be an integers and $-D < 0$ a discriminant which is not a square in $\mathbb{Z}/N\mathbb{Z}$. Then the set $\mathcal{Q}^{(N)}_{-D}$ is empty. In particular, we have that $\mathrm{Tr}^{(N)}_{-D}(f) = H^{(N)}(D) = 0$ for any $\Gamma_0(N)$-invariant function f.*

Proof. A quadratic form $[a, b, c] \in \mathcal{Q}^{(N)}_{-D}$ satisfies $-D = b^2 - 4ac$ and $N|a$, hence if $-D$ is not a square modulo N, there cannot be any such forms. □

6.1. Proof of Theorem 1.2.

Suppose first that $p \in \{5, 7\}$ and let D be as in Theorem 1.2. The congruences in Appendix C together with the identities in Appendix D imply the congruence

$$\dim(W_D) \equiv \mathrm{tr}(g_p|W_D) \equiv \mathrm{Tr}^{(p)}_4(D) - 24H(D) + \alpha_p H^{(p)}(D) \pmod p$$

for some integer α_p. By Lemma 6.1, the terms $\mathrm{Tr}_4^{(p)}(D)$ and $H^{(p)}(D)$ vanish for D as required, proving the result. For $p=3$, one replaces the modulus above by 3^2, making the congruence non-trivial.

For $p=2$, we note that there is a congruence between $\dim W_D$ and $\mathrm{tr}(g_2|W_D)$ modulo 2^{11} by Appendix C. As one easily sees through a Sturm bound argument, we also have

$$\dim W_D \equiv \mathrm{tr}(g_2|W_D) \equiv 0 \pmod{16}$$

for $D \equiv 4, 8 \pmod{16}$, which is the case in particular when $-D < 8$ is an even fundamental discriminant. The fact that for these D the class number is even can be seen in various ways, for example by noting that by a famous theorem of Gauss and Hermite we have that $24H(D) = 2r_3(D/4)$, where $r_3(n)$ is the number of representations of n as the sum of three squares. Since $-D$ is fundamental, it follows that $D/4$ is square-free and hence is not the sum of three or just two equal squares. Through an easy case-by-case analysis one then finds that $r_3(D/4)$ is always divisible by 8. Alternatively, one could also show the modular forms congruence

$$\sum_{n\equiv 1,2 \pmod 4} r_3(n)q^n \equiv 6\sum_{n=0}^{\infty} q^{(2n+1)^2} + 4\sum_{n=0}^{\infty} q^{2(2n+1)^2} \pmod 8.$$

This completes the proof.

6.2. **Preliminaries on Elliptic Curves.** The proofs of Theorems 1.3 and 1.4 require a little preparation which we provide in this section.

One of the most important open problems in the context of elliptic curves is certainly the Birch and Swinnerton-Dyer Conjecture.

Conjecture 6.2. *Let $E/\mathbb{Q}$ be an elliptic curve. Then we have that*

$$\frac{L^{(r)}(E,1)}{r!\Omega_E} = \frac{\#\text{Ш}(E)\cdot \mathrm{Reg}(E)\prod_\ell c_\ell(E)}{(\#E(\mathbb{Q})_{tors})^2}, \tag{6.1}$$

where r denotes the order of vanishing of $L(E,s)$ at $s=1$, which equals the Mordell–Weil rank of E, Ω_E is the real period of E, $\mathrm{Reg}(E)$ denotes the regulator of the curve, the $c_\ell(E)$ for prime ℓ are the Tamagawa numbers of E, and, finally, $\#E(\mathbb{Q})_{tors}$ signifies the torsion subgroup of the $\mathbb{Q}$-rational points of E.

The weak Birch and Swinnerton-Dyer conjecture—that the order of vanishing of $L(E,s)$ at $s=1$ equals the rank of E—was established for curves of ranks 0 and 1 through work of Gross–Zagier [47] and Kolyvagin [54]. More recently, Bhargava–Shankar [5] proved, using Kolyvagin's theorem and the proof of the Iwasawa main conjectures for GL_2 by Skinner–Urban [69] (among other deep results), that a positive proportion of all elliptic curves satisfy the weak Birch and Swinnerton-Dyer Conjecture.

It is known that the left-hand side of (6.1) is always a rational number, see for instance [2, Theorem 3.2]. The following result shows that in certain situations, a local version of Conjecture 6.2, which is going to be sufficient for our purposes, holds.

Theorem 6.3 ([68], Theorem C)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and $p \geq 3$ a prime of good ordinary or multiplicative reduction. Further assume that the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-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

$$\operatorname{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right) = \operatorname{ord}_p\left(\#\text{Ш}(E)\prod_\ell c_\ell(E)\right).$$

If $L(E,1) = 0$, then we have $\mathrm{Sel}(E)[p] \neq \{0\}$.

We are especially interested in quadratic twists of elliptic curves. In this context, the following result by Agashe, giving the real period of such a twist, turns out to be very useful.

Lemma 6.4 ([3], Lemma 2.1)**.** *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and let $-D < 0$ be a fundamental discriminant coprime to N. Then we have that*

$$\Omega_{E(-D)} = c_E \cdot c_\infty(E(-D)) \cdot \omega_-(E)/\sqrt{D},$$

where c_E denotes the Manin constant of E, $c_\infty(E(-D))$ denotes the number of components of $E(-D)$ over $\mathbb{R}$, and $\omega_-(E)$ denotes the second period of the period lattice of E.

Remark. The famous Manin Conjecture states that $c_E = 1$.

Combining this with a theorem of Kohnen [53] (cf. Proposition 4.4), we obtain the following.

Lemma 6.5. *Let $E/\mathbb{Q}$ be an elliptic curve of odd, square-free conductor N and let $-D < 0$ be a fundamental discriminant satisfying $\left(\frac{-D}{\ell}\right) = w_\ell$, where w_ℓ denotes the eigenvalue of the newform $F_E \in S_2(\Gamma_0(N))$ associated to E and the Atkin–Lehner involution W_ℓ, $\ell|N$. Denote by D_0 the smallest such discriminant. Further let $f_E(\tau) = \sum_{n=3}^\infty b_E(n)q^n \in S^+_{\frac{3}{2}}(\Gamma_0(4N))$ be the weight $3/2$ cusp form associated to F_E under the Shintani lift. For $p \geq 3$ prime we then have that*

$$\operatorname{ord}_p\left(\frac{L(E(-D),1)}{\Omega_{E(-D)}}\right) = \operatorname{ord}_p\left(\frac{L(E(-D_0),1)}{\Omega_{E(-D_0)}}\right) + \operatorname{ord}_p\left(b_E(|D|)^2\right).$$

Proof. By combining Proposition 4.4 and Lemma 6.4, we find for the fundamental discriminants $-D < 0$ as in the lemma that

$$\frac{L(E(-D),1)}{\Omega_{E(-D)}} = \frac{\pi\langle F,F\rangle}{c_E \cdot c_\infty(E(-D))2^{\omega(N)}\langle f,f\rangle\omega_-(E)} \cdot |b_E(D)|^2. \tag{6.2}$$

We see that the only quantities in this formula depending on D are $c_\infty(E(-D))$ and $b_E(D)$. Since the former is always either 1 or 2 and p is odd, it doesn't affect the p-adic valuation at all, which proves the lemma. □

Remark. If the conductor N is even but still square-free, the same result still holds along the same lines, using the remark following Proposition 4.4. The exact formula in this case only differs from (6.2) by a power of 2, which doesn't affect the p-adic valuation.

6.3. **Proofs.** In this section, we prove Theorems 1.3 and 1.4. The proofs of both theorems are very similar in their main steps, so we combine them here.

Proof of Theorems 1.3 and 1.4. By applying the expressions for the relevant $F_{[g]}$ in terms of traces of singular moduli, class numbers and weight 3/2 cusp forms in Appendix D, and the congruences in Appendix C, we find that

$$\begin{aligned}
\dim(W_D) \equiv \operatorname{tr}(g_{11}|W_D) &\equiv \operatorname{Tr}_4^{(11)}(D) - 24H(D) + \alpha_{11}H^{(11)}(D) + \gamma_{11}b_{11}(D) \pmod{11},\\
\operatorname{tr}(g_2|W_D) \equiv \operatorname{tr}(g_{14}|W_D) &\equiv \operatorname{Tr}_4^{(14)}(D) + \delta_7(H(D) - \delta_7 H^{(2)}(D))\\
&\qquad + \alpha_7 H^{(7)}(D) + \beta_7 H^{(14)}(D) + \gamma_7 b_{14}(D) \pmod{7},\\
\operatorname{tr}(g_3|W_D) \equiv \operatorname{tr}(g_{15}|W_D) &\equiv \operatorname{Tr}_4^{(15)}(D) + \delta_5(H(D) - \delta_5 H^{(3)}(D))\\
&\qquad + \alpha_5 H^{(5)}(D) + \beta_5 H^{(15)}(D) + \gamma_5 b_{15}(D) \pmod{5},\\
\dim(W_D) \equiv \operatorname{tr}(g_{19}|W_D) &\equiv \operatorname{Tr}_4^{(19)}(D) - 24H(D) + \alpha_{19}H^{(19)}(D) + \gamma_{19}b_{19}(D) \pmod{19},
\end{aligned}$$

where $\delta_p = \frac{p-1}{2}$, α_p, β_p are some integers, γ_p are p-adic units, and $b_N(D)$ denotes the D^{th} coefficient of the weight 3/2 cusp form $\mathscr{G}^{(N)}$ specified in Appendix D. If $-D$ is a fundamental discriminant as specified in Theorems 1.3 and 1.4 respectively, then by Lemma 6.1, the terms $\operatorname{Tr}_4^{(N)}(D)$ as well as $H^{(p)}(D)$ and $H^{(N)}(D)$ above disappear. This shows that the class number congruences in our theorems hold if and only if p divides the coefficient $b_N(D)$, i.e. by Lemma 6.5[4] if and only if $\operatorname{ord}_p\left(\frac{L(E_N(-D),1)}{\Omega_{E_N(-D)}}\right) > 0$.

Suppose for simplicity that $L(E_N(-D),1) \neq 0$. According to the Birch and Swinnerton-Dyer Conjecture 6.2, this implies that

$$\operatorname{ord}_p(\#\text{Ш}(E_N(-D))\prod_\ell c_\ell(E(-D))) > 0,$$

so our theorems follow, conditionally on Conjecture 6.2, if the Tamagawa numbers $c_\ell(E(-D))$ are never divisible by p in our cases. To establish this, we note (cf. [67, Appendix C, Table 15.1]) that for an elliptic curve $E/\mathbb{Q}$ we have that $p|c_\ell(E)$ if and only if the reduction type of E at ℓ is I_n with $p|n$, which means that $\operatorname{ord}_\ell(\Delta(E)) = n$, where $\Delta(E)$ denotes the (minimal) discriminant of E. An inspection of Tate's algorithm for the computation of Tamagawa numbers and the well-known formulas for minimal discriminants from the Kraus–Laska algorithm reveals that in our case, because we are considering twists of elliptic curves by fundamental discriminants, all the Tamagawa numbers must be in $\{1,2,3,4\}$. The argumentation in the case $L(E(-D),1) = 0$ is similar. This completes the proof of Theorem 1.3 for $N \in \{11, 19\}$.

The truth of Theorem 1.4 does not depend on the Birch and Swinnerton-Dyer Conjecture, but rather on Skinner's Theorem 6.3. A lemma of Serre [65, §2.8, Corollaire, p. 284] shows that the Galois representations $E_{14}(-D)[7]$ and $E_{15}(-D)[5]$ are surjective and hence irreducible. Furthermore, it is immediate to check that $E_{14}(-D)$ (resp. $E_{15}(-D)$) has

[4]A Magma computation reveals that the ratio $\frac{L(E_N(-D_0),1)}{\Omega_{E_N(-D_0)}}$ for the smallest possible D_0 in each case is a p-adic unit.

multiplicative reduction modulo 2 (resp. 3) and that $E_{14}(-D)[7]$ (resp. $E_{15}(-D)[5]$) ramifies there, so the conditions of Theorem 6.3 are satisfied, completing the proof of Theorem 1.4. $\square$

7. Examples

Here we offer some numerical examples which illustrate the congruences described in the introduction.

7.1. **Class Number Congruences.** Here are example class number congruences that arise from Theorem 1.2. Recall that this theorem offers congruences modulo 16, 9, 5, and 7 for certain fundamental discriminants $-D < 0$ which satisfy given congruence conditions. The three columns in Tables 7.1 to 7.4 are congruent, which illustrates the theorem.

D	$\dim W_D$	$\mathrm{tr}(g_2\|W_D)$	$-24H(D)$
20	$798588584512 \equiv 0 \pmod{16}$	$576 \equiv 0 \pmod{16}$	$-48 \equiv 0 \pmod{16}$
24	$116700...6880 \equiv 0 \pmod{16}$	$-1088 \equiv 0 \pmod{16}$	$-48 \equiv 0 \pmod{16}$
40	$905977...8912 \equiv 0 \pmod{16}$	$-10304 \equiv 0 \pmod{16}$	$-48 \equiv 0 \pmod{16}$

Table 7.1. $p = 2$

D	$\dim W_D$	$\mathrm{tr}(g_3\|W_D)$	$-24H(D)$
4	$143376 \equiv 6 \pmod{9}$	$6 \equiv 6 \pmod{9}$	$-12 \equiv 6 \pmod{9}$
7	$8288256 \equiv 3 \pmod{9}$	$12 \equiv 3 \pmod{9}$	$-24 \equiv 3 \pmod{9}$
19	$392037661056 \equiv 3 \pmod{9}$	$12 \equiv 3 \pmod{9}$	$-24 \equiv 3 \pmod{9}$
31	$779869748441088 \equiv 0 \pmod{9}$	$36 \equiv 0 \pmod{9}$	$-72 \equiv 0 \pmod{9}$

Table 7.2. $p = 3$

D	$\dim W_D$	$\mathrm{tr}(g_5\|W_D)$	$-24H(D)$
3	$26752 \equiv 2 \pmod{5}$	$2 \equiv 2 \pmod{5}$	$-8 \equiv 2 \pmod{5}$
7	$8288256 \equiv 1 \pmod{5}$	$6 \equiv 1 \pmod{5}$	$-24 \equiv 1 \pmod{5}$
23	$6103910176768 \equiv 3 \pmod{5}$	$18 \equiv 3 \pmod{5}$	$-72 \equiv 3 \pmod{5}$
47	$2548919136928993280 \equiv 0 \pmod{5}$	$30 \equiv 0 \pmod{5}$	$-120 \equiv 0 \pmod{5}$

Table 7.3. $p = 5$

D	$\dim W_D$	$\mathrm{tr}(g_7\|W_D)$	$-24H(D)$
4	$143376 \equiv 2 \pmod{7}$	$2 \equiv 2 \pmod{7}$	$-12 \equiv 2 \pmod{7}$
8	$26124256 \equiv 4 \pmod{7}$	$4 \equiv 4 \pmod{7}$	$-24 \equiv 4 \pmod{7}$
11	$561346944 \equiv 4 \pmod{7}$	$4 \equiv 4 \pmod{7}$	$-24 \equiv 4 \pmod{7}$
15	$18508941312 \equiv 1 \pmod{7}$	$8 \equiv 1 \pmod{7}$	$-48 \equiv 1 \pmod{7}$
71	$4918685030138843868979 2 \equiv 0 \pmod{7}$	$28 \equiv 0 \pmod{7}$	$-168 \equiv 0 \pmod{7}$

Table 7.4. $p = 7$

7.2. **Selmer and Tate–Shafarevich Group Congruences.** Theorems 1.3 and 1.4 offer criteria for detecting elements in p-Selmer groups and Tate–Shafarevich groups of quadratic twists of certain elliptic curves. Theorem 1.3 assumes the truth of the Birch and Swinnerton-Dyer Conjecture. Theorem 1.4 is unconditional thanks to results of Skinner–Urban.

Here we offer data related to the curves E_{14} and E_{15}. In the notation of Theorem 1.4, we consider fundamental discriminants $-D$ such that $\left(\frac{-D}{p}\right) = -1$ and $\left(\frac{-D}{p'}\right) = 1$. For convenience let

$$\begin{aligned} H_{14}(D) &:= \delta_7(H(D) - \delta_7 H^{(2)}(D)), & H_{15}(D) &:= \delta_5(H(D) - \delta_5 H^{(3)}(D)),\\ \mathrm{tr}_2(D) &:= \mathrm{tr}(g_2|W_D), & \mathrm{tr}_3(D) &:= \mathrm{tr}(g_3|W_D),\\ \mathrm{Diff}_{14}(D) &:= H_{14}(D) - \mathrm{tr}_2(D), & \mathrm{Diff}_{15}(D) &:= H_{15}(D) - \mathrm{tr}_3(D). \end{aligned}$$

We have the following numerics[5]. In Tables 7.5 and 7.6, the second and third columns offer graded traces and differences of class numbers. The fourth and fifth columns offer Mordell–Weil ranks and orders of Tate–Shafarevich groups assuming the Birch and Swinnerton-Dyer Conjecture. By Theorem 1.4, these columns are congruent if and only the corresponding p-Selmer group is nontrivial. First note that if these two columns are incongruent, then both the Mordell–Weil rank over $\mathbb{Q}$ and the p-part of the Tate–Shafarevich groups are trivial. However, when these columns are congruent, notice that either the rank is positive or the Tate–Shafarevich group is nontrivial at p.

D	$\mathrm{tr}_2(D)$	$H_{14}(D)$	$\mathrm{Diff}_{14}(D) \pmod 7$	$\mathrm{rk}(E_{14}(-D))$	$\#Ш_{an}(E_{14}(-D))$
15	-96256	-30	3	0	1
23	-1746944	-45	0	2	1
39	-165767168	-60	4	0	1
71	-156822906880	-105	4	0	1
79	-669595144192	-75	3	0	1
239	-6190369...040	-225	0	2	1
2671	-1630362...664	-345	0	0	49

TABLE 7.5. Examples for the curve E_{14}

[5]The authors would like to thank Drew Sutherland for computing the elliptic curve invariants in Tables 7.5 and 7.6.

D	$\mathrm{tr}_3(D)$	$H_{15}(D)$	$\mathrm{Diff}_{15}(D) \pmod 5$	$\mathrm{rk}(E_{15}(-D))$	$\#Ш_{an}(E_{15}(-D))$
8	-188	-6	3	0	1
23	-11456	-18	2	0	1
47	-860032	-30	3	0	1
68	-15834144	-24	0	2	1
83	-96763256	-18	2	0	1
248	-10546706...288	-48	0	2	1
308	-45931281...288	-48	0	2	1
587	-54506997...592	-42	0	0	25
1523	-15706167...792	-42	0	0	25

TABLE 7.6. Examples for the curve E_{15}

Appendix A. The Character Table of $O'N$

Here we give the character table of the O'Nan group $O'N$ over the complex numbers. For $n \in \mathbb{N}$ we let $\zeta_n := e^{\frac{2\pi i}{n}}$ and define

$$A := \frac{1+3\sqrt{5}}{2}, \qquad B := \sqrt{2},$$
$$C := -\zeta_{19} - \zeta_{19}^{7} - \zeta_{19}^{8} - \zeta_{19}^{11} - \zeta_{19}^{12} - \zeta_{19}^{18},$$
$$D := -\zeta_{19}^{4} - \zeta_{19}^{6} - \zeta_{19}^{9} - \zeta_{19}^{10} - \zeta_{19}^{13} - \zeta_{19}^{15},$$
$$E := -\zeta_{19}^{2} - \zeta_{19}^{3} - \zeta_{19}^{5} - \zeta_{19}^{14} - \zeta_{19}^{16} - \zeta_{19}^{17},$$
$$F := i\sqrt{5}, \qquad G := \sqrt{7}, \qquad H := \frac{-1+i\sqrt{31}}{2}.$$

We use $\overline{A}$, $\overline{B}$, &c. to denote images under the obvious Galois involutions. Note that C, D, and E are in one Galois orbit as well, since

$$(X-C)(X-D)(X-E) = X^3 - X^2 - 6X + 7.$$

The character table is reproduced from Gap4 [41].

	$1A$	$2A$	$3A$	$4A$	$4B$	$5A$	$6A$	$7A$	$7B$	$8A$	$8B$	$10A$	$11A$	$12A$	$14A$	$15A$	$15B$	$16A$	$16B$	$16C$	$16D$	$19A$	$19B$	$19C$	$20A$	$20B$	$28A$	$28B$	$31A$	$31B$
χ_1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
χ_2	10944	64	9	64	0	-1	1	17	3	0	0	-1	-1	1	1	-1	-1	0	0	0	0	0	0	0	-1	-1	1	1	1	1
χ_3	13376	-64	11	64	0	1	-1	-1	-1	0	0	1	0	1	-1	1	1	0	0	0	0	0	0	0	-1	-1	1	1	H	$\overline{H}$
χ_4	13376	-64	11	64	0	1	-1	-1	-1	0	0	1	0	1	-1	1	1	0	0	0	0	0	0	0	-1	-1	1	1	$\overline{H}$	H
χ_5	25916	-36	-4	20	4	1	0	-5	2	0	0	-1	0	2	-1	1	1	0	0	0	0	0	0	0	F	$-F$	-1	-1	0	0
χ_6	25916	-36	-4	20	4	1	0	-5	2	0	0	-1	0	2	-1	1	1	0	0	0	0	0	0	0	$-F$	F	-1	-1	0	0
χ_7	26752	128	22	0	0	2	2	-2	-2	0	0	-2	0	0	2	2	2	0	0	0	0	0	0	0	0	0	0	0	-1	-1
χ_8	32395	75	-5	35	3	0	3	6	-1	3	-1	0	0	-1	-2	0	0	1	1	-1	-1	0	0	0	0	0	0	0	0	0
χ_9	32395	75	-5	35	3	0	3	6	-1	-1	3	0	0	-1	-2	0	0	-1	-1	1	1	0	0	0	0	0	0	0	0	0
χ_{10}	37696	-64	31	-64	0	1	-1	15	1	0	0	1	-1	-1	-1	1	1	0	0	0	0	0	0	0	1	1	-1	-1	0	0
χ_{11}	52668	92	18	20	4	-2	2	-7	0	0	0	2	0	2	1	-2	-2	0	0	0	0	0	0	0	0	0	-1	-1	-1	-1
χ_{12}	58311	71	-9	71	7	1	-1	1	1	-1	-1	1	0	-1	1	1	1	-1	-1	-1	-1	0	0	0	1	1	1	1	0	0
χ_{13}	58311	71	-9	-1	-1	1	-1	1	1	3	-1	1	0	-1	1	1	1	-1	-1	1	1	0	0	0	-1	-1	-1	-1	0	0
χ_{14}	58311	71	-9	-1	-1	1	-1	1	1	-1	3	1	0	-1	1	1	1	1	1	-1	-1	0	0	0	-1	-1	-1	-1	0	0
χ_{15}	58653	-35	9	-35	-3	8	1	0	0	1	1	0	1	1	0	-1	-1	-1	-1	-1	-1	0	0	0	0	0	0	0	1	1
χ_{16}	64790	70	-10	-70	2	0	-2	12	-2	0	0	0	0	2	0	0	0	B	$-B$	$-B$	B	0	0	0	0	0	0	0	0	0
χ_{17}	64790	70	-10	-70	2	0	-2	12	-2	0	0	0	0	2	0	0	0	$-B$	B	B	$-B$	0	0	0	0	0	0	0	0	0
χ_{18}	85064	-56	14	-56	8	-1	-2	0	0	0	0	-1	1	-2	0	-1	-1	0	0	0	0	1	1	1	-1	-1	0	0	0	0
χ_{19}	116963	35	-1	35	3	8	-1	0	0	-1	-1	0	0	-1	0	-1	-1	1	1	1	1	-1	-1	-1	0	0	0	0	0	0
χ_{20}	143374	14	4	126	-2	-1	-4	0	0	2	2	-1	0	0	0	-1	-1	0	0	0	0	0	0	0	1	1	0	0	-1	-1
χ_{21}	169290	90	0	-90	-2	0	0	-5	2	0	0	0	0	0	-1	0	0	B	$-B$	B	$-B$	0	0	0	0	0	1	1	-1	-1
χ_{22}	169290	90	0	-90	-2	0	0	5	2	0	0	0	0	0	-1	0	0	$-B$	B	$-B$	B	0	0	0	0	0	1	1	-1	-1
χ_{23}	175616	0	8	0	0	-4	0	0	0	0	0	0	1	0	0	A	$\overline{A}$	0	0	0	0	-1	-1	-1	0	0	0	0	1	1
χ_{24}	175616	0	8	0	0	-4	0	0	0	0	0	0	1	0	0	$\overline{A}$	A	0	0	0	0	-1	-1	-1	0	0	0	0	1	1
χ_{25}	175770	90	0	90	-6	0	0	7	0	2	-2	0	1	0	-1	0	0	0	0	0	0	1	1	1	0	0	-1	-1	0	0
χ_{26}	207360	0	0	0	0	0	0	-8	-1	0	0	0	-1	0	0	0	0	0	0	0	0	C	E	D	0	0	0	0	1	1
χ_{27}	207360	0	0	0	0	0	0	-8	-1	0	0	0	-1	0	0	0	0	0	0	0	0	D	C	E	0	0	0	0	1	1
χ_{28}	207360	0	0	0	0	0	0	-8	-1	0	0	0	-1	0	0	0	0	0	0	0	0	E	D	C	0	0	0	0	1	1
χ_{29}	234080	-160	-10	0	0	0	2	7	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	G	$-G$	-1	-1
χ_{30}	234080	-160	-10	0	0	0	2	7	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	$-G$	G	-1	-1

TABLE A.1. Character table of $O'N$

Appendix B. Multiplicities of Irreducible Representations in W

We denote by V_j the $O'N$-module corresponding to the irreducible χ_j in Table A.1.

The following table gives the multiplicities of V_j in the (virtual) modules W_m in Theorem 4.1. Negative multiplicities are printed in bold.

m	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8	V_9	V_{10}
3	0	0	0	0	0	0	1	0	0	0
4	1	0	0	0	0	0	0	0	0	0
7	0	0	1	1	1	1	**-2**	0	0	2
8	**-2**	1	0	0	2	2	0	2	2	1
11	0	18	8	8	28	28	40	48	48	34
12	**-1**	33	44	44	76	76	88	98	98	122
15	0	406	581	581	1061	1061	1010	1252	1252	1568
16	0	978	1193	1193	2316	2316	2386	2892	2892	3362
19	2	9484	11205	11205	21948	21948	23114	27766	27766	31894
20	5	18951	23161	23161	44930	44930	46322	56156	56156	65271
23	2	144238	177831	177831	343685	343685	352892	428308	428308	499900
24	25	277191	338794	338794	656282	656282	677588	820362	820362	954783
27	212	1795740	2189365	2189365	4245047	4245047	4388491	5310882	5310882	6174470
28	286	3264537	3989983	3989983	7730566	7730566	7979966	9663217	9663217	11244510
31	1562	18513448	22644956	22644956	43863830	43863830	45258570	54815104	54815104	63803360
32	2964	32416998	39620773	39620773	76765848	76765848	79241546	95957290	95957290	111658534
35	15432	165271652	201946677	201946677	391304807	391304807	403986962	489174874	489174874	569165006
36	25645	279985728	342204752	342204752	663020690	663020690	684409504	828775828	828775828	964395212

Table B.1. Multiplicities, part I.

m	V_{11}	V_{12}	V_{13}	V_{14}	V_{15}	V_{16}	V_{17}	V_{18}	V_{19}	V_{20}
3	0	0	0	0	0	0	0	0	0	0
4	0	1	0	0	0	0	0	1	0	0
7	0	0	0	0	2	0	0	2	2	2
8	2	2	4	4	3	4	4	2	7	8
11	72	80	80	80	64	88	88	96	144	176
12	164	173	178	178	185	197	197	261	359	444
15	2068	2296	2296	2296	2384	2556	2556	3458	4680	5754
16	4704	5208	5200	5200	5222	5782	5782	7598	10434	12788
19	45058	49802	49802	49802	49804	55314	55314	72214	99604	122014
20	91248	101087	101068	101068	101628	112302	112302	147407	202710	248454
23	696576	771644	771644	771644	777260	857476	857476	1127304	1548902	1898946
24	1333868	1476646	1476680	1476680	1485435	1640744	1640744	2154259	2962056	3630946
27	8633536	9557140	9557140	9557140	9609292	10618702	10618702	13936084	19166220	23493012
28	15710534	17393789	17393848	17393848	17495886	19326474	19326474	25374046	34889374	42767664
31	89122420	98675012	98675012	98675012	99266748	109640000	109640000	143966514	197940198	242639964
32	156007392	172723130	172723024	172723024	173735638	191914504	191914504	251967626	346455812	424687592
35	795291752	880491400	880491400	880491400	885616006	978320518	978320518	1284400160	1766091974	2164876128
36	1347430236	1491796517	1491796318	1491796318	1500546542	1657551544	1657551544	2176231689	2992317414	3668002182

Table B.2. Multiplicities, part II.

m	V_{21}	V_{22}	V_{23}	V_{24}	V_{25}	V_{26}	V_{27}	V_{28}	V_{29}	V_{30}
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
7	2	2	3	3	2	4	4	4	6	6
8	10	10	9	9	10	12	12	12	14	14
11	216	216	214	214	224	252	252	252	270	270
12	521	521	543	543	542	638	638	638	718	718
15	6746	6746	7057	7057	7006	8328	8328	8328	9492	9492
16	15102	15102	15671	15671	15680	18500	18500	18500	20884	20884
19	144268	144268	149402	149402	149782	176414	176414	176414	198703	198703
20	293374	293374	304323	304323	304596	359352	359352	359352	405676	405676
23	2241422	2241422	2326161	2326161	2327256	2746666	2746666	2746666	3102368	3102368
24	4287248	4287248	4447476	4447476	4451367	5251357	5251357	5251357	5927992	5927992
27	27742332	27742332	28775511	28775511	28804106	33976834	33976834	33976834	38348849	38348849
28	50498270	50498270	52385258	52385258	52431245	61854317	61854317	61854317	69824744	69824744
31	286490080	286490080	297207048	297207048	297456630	350929578	350929578	350929578	396169260	396169260
32	501453364	501453364	520191449	520191449	520647692	614220424	614220424	614220424	693367868	693367868
35	2556221884	2556221884	2651707883	2651707883	2654066434	3131025718	3131025718	3131025718	3534425359	3534425359
36	4331022760	4331022760	4492864127	4492864127	4496803456	5304984880	5304984880	5304984880	5988574304	5988574304

TABLE B.3. Multiplicities, part III.

APPENDIX C. CONGRUENCES

$\underline{p=31}$:

$$0 \equiv F_{1A} - F_{31AB} \pmod{31}$$

$\underline{p=19}$:

$$0 \equiv F_{1A} - F_{19ABC} \pmod{19}$$

$\underline{p=11}$:

$$0 \equiv F_{1A} - F_{11A} \pmod{11}$$

$\underline{p=7}$:

$$\begin{aligned} 0 &\equiv F_{1A} - F_{7AB} && \pmod{7^3} \\ &\equiv F_{2A} - F_{14A} && \pmod{7} \\ &\equiv F_{4AB} - F_{28AB} && \pmod{7} \end{aligned}$$

$\underline{p=5}$:

$$\begin{aligned} 0 &\equiv F_{1A} - F_{5A} && \pmod{5^3} \\ &\equiv F_{2A} - F_{10A} && \pmod{5} \\ &\equiv F_{3A} - F_{15AB} && \pmod{5} \\ &\equiv F_{4AB} - F_{20AB} && \pmod{5} \end{aligned}$$

$\underline{p=3:}$

$$\begin{aligned}
0 &\equiv F_{1A} - F_{3A} && \pmod{3^5}\\
&\equiv F_{2A} - F_{6A} && \pmod{3^2}\\
&\equiv F_{4AB} - F_{12A} && \pmod{3^2}\\
&\equiv F_{5A} - F_{15AB} && \pmod{3^2}
\end{aligned}$$

$\underline{p=2:}$

$$\begin{aligned}
0 &\equiv F_{1A} + 303F_{2A} + 3024F_{4AB} + 4864F_{8AB} + 57344F_{16ABCD} && \pmod{2^{16}}\\
&\equiv F_{2A} + 7F_{4AB} + 8F_{8AB} + 112F_{16ABCD} && \pmod{2^7}\\
&\equiv F_{3A} + F_{6A} + 6F_{12A} && \pmod{2^3}\\
&\equiv F_{4AB} + F_{8AB} + 14F_{16ABCD} && \pmod{2^4}\\
&\equiv F_{5A} + F_{10A} + 6F_{20AB} && \pmod{2^3}\\
&\equiv F_{6A} + F_{12A} && \pmod{2}\\
&\equiv F_{7AB} + F_{14AB} && \pmod{2^3}\\
&\equiv F_{8AB} + 7F_{16ABCD} && \pmod{2^3}\\
&\equiv F_{10A} + F_{20AB} && \pmod{2}\\
&\equiv F_{14A} + F_{28AB} && \pmod{2}
\end{aligned}$$

Appendix D. Traces of Singular Moduli

We give the explicit descriptions of $F_{[g]}$ in terms of traces of singular moduli and class numbers as described in Section 5.

$$\begin{aligned}
F_{1A} &= \mathscr{T}^{(1)},\\
F_{2A} &= \mathscr{T}^{(2)} + 12\mathscr{H}^{(1)} - 12\mathscr{H}^{(2)},\\
F_{3A} &= \mathscr{T}^{(3)} + 12\mathscr{H}^{(1)} - 12\mathscr{H}^{(3)},\\
F_{4AB} &= \mathscr{T}^{(4)} + 12\mathscr{H}^{(2)} - 12\mathscr{H}^{(4)},\\
F_{5A} &= \mathscr{T}^{(5)} + 6\mathscr{H}^{(1)} - 6\mathscr{H}^{(5)},\\
F_{6A} &= \mathscr{T}^{(6)} - 12\mathscr{H}^{(1)} + 8\mathscr{H}^{(2)} + \frac{21}{2}\mathscr{H}^{(3)} - \frac{13}{2}\mathscr{H}^{(6)},\\
F_{7AB} &= \mathscr{T}^{(7)} + 4\mathscr{H}^{(1)} - 4\mathscr{H}^{(7)},\\
F_{8AB} &= \mathscr{T}^{(8)} + 4\mathscr{H}^{(4)} - 4\mathscr{H}^{(8)},\\
F_{10A} &= \mathscr{T}^{(10)} - 6\mathscr{H}^{(1)} + +4\mathscr{H}^{(2)} + \frac{11}{2}\mathscr{H}^{(5)} - \frac{7}{2}\mathscr{H}^{(10)},\\
F_{11A} &= \mathscr{T}^{(11,+)} + \frac{12}{5}\mathscr{H}^{(1)} - \frac{6}{5}\mathscr{H}^{(11)} - \frac{4}{5}\mathscr{G}^{(11)},\\
F_{12A} &= \mathscr{T}^{(12)} - 4\mathscr{H}^{(2)} + 4\mathscr{H}^{(4)} + \frac{5}{2}\mathscr{H}^{(6)} - \frac{5}{2}\mathscr{H}^{(12)},\\
F_{14A} &= \mathscr{T}^{(14,+)} - 4\mathscr{H}^{(1)} + \frac{8}{3}\mathscr{H}^{(2)} + \frac{15}{4}\mathscr{H}^{(7)} - \frac{41}{24}\mathscr{H}^{(14)} + \frac{8}{3}\mathscr{G}^{(14)},\\
F_{15AB} &= \mathscr{T}^{(15,+)} - 3\mathscr{H}^{(1)} + \frac{9}{4}\mathscr{H}^{(3)} + \frac{5}{2}\mathscr{H}^{(5)} - \frac{13}{8}\mathscr{H}^{(15)} + \frac{9}{4}\mathscr{G}^{(15)},\\
F_{16ABCD} &= \mathscr{T}^{(16)} + 2\mathscr{H}^{(8)} - 2\mathscr{H}^{(16)},\\
F_{19ABC} &= \mathscr{T}^{(19,+)} + \frac{4}{3}\mathscr{H}^{(1)} - \frac{2}{3}\mathscr{H}^{(19)} + \frac{4}{3}\mathscr{G}^{(19)},\\
F_{20AB} &= \mathscr{T}^{(20,+)} - 2\mathscr{H}^{(2)} + 2\mathscr{H}^{(4)} + \frac{3}{2}\mathscr{H}^{(10)} - \frac{3}{2}\mathscr{H}^{(20)},\\
F_{28AB} &= \mathscr{T}^{(28,+)} - \frac{4}{3}\mathscr{H}^{(2)} + \frac{4}{3}\mathscr{H}^{(4)} + \frac{25}{24}\mathscr{H}^{(14)} - \frac{25}{24}\mathscr{H}^{(28)} + \frac{8}{3}\mathscr{G}^{(28)},\\
F_{31AB} &= \mathscr{T}^{(31,+)} + \frac{4}{5}\mathscr{H}^{(1)} - \frac{2}{5}\mathscr{H}^{(31)} + \frac{3}{5}\mathscr{G}^{(31)}.
\end{aligned}$$

Here, $\mathscr{G}^{(N)}$ denotes the unique weight $3/2$ cusp form for $\Gamma_0(4N)$ in the plus space with leading coefficient 1 if $N < 28$, $\mathscr{G}^{(28)}$ is the unique normalized cusp form in $S_{\frac{3}{2}}(\Gamma_0(28))$ hit with the V_4-operator, and $\mathscr{G}^{(31)} \in S^+_{\frac{3}{2}}(\Gamma_0(124))$ is the unique cusp form in this space satisfying

$$\mathscr{G}^{(31)}(\tau) = q^4 + \frac{11}{3}q^7 + O(q^8).$$

There is exactly one newform $f^{(31)}$ in $S^+_{\frac{3}{2}}(\Gamma_0(124))$ up to Galois conjugation and we have

$$f^{(31)}(\tau) = q^4 - \frac{1+\sqrt{5}}{2}q^7 - \frac{1-\sqrt{5}}{2}q^8 + \frac{1+\sqrt{5}}{2}q^{16} + O(q^{20}),$$

so that we can express $g^{(31)}$ in terms of this newform as follows,

$$\mathscr{G}^{(31)}(\tau) = \frac{3+5\sqrt{5}}{6}f^{(31)}(\tau) + \frac{3-5\sqrt{5}}{6}f^{(31)^\sigma}(\tau),$$

where, as in Table 5.2, a superscript σ denotes Galois conjugation.

References

[1] M. Aschbacher, *The status of the classification of the finite simple groups*, Notices Amer. Math. Soc. **51** (2004), no. 7, 736–740. MR 2072045

[2] A. Agashe, *A visible factor of the special L-value*, J. Reine Angew. Math. **644** (2010), 159–187.

[3] ______, *Squareness of the special L-values of twists*, Int. J. Number Theory **6** (2010), no. 5, 1091–1111.

[4] L. Beneish and H. Larson, *Traces of singular values of hauptmoduln*, Int. J. Number Theory **11** (2015), 1027–1048.

[5] M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants and the proof of a positive proportion of elliptic curves having rank* 0, Ann. Math. **181** (2015), no. 2, 587–621.

[6] R. E. Borcherds, *Monstrous moonshine and monstrous Lie superalgebras*, Invent. Math. **109** (1992), no. 2, 405–444.

[7] ______, *Automorphic forms on $O_{s+2,2}(\mathbb{R})$ and infinite products*, Invent. Math. **120**, (1995), 161-213.

[8] W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system. I The user language*, J. Symbolic Comput., **24** (1997), no. 3–4, 235–265.

[9] K. Bringmann, A. Folsom, K. Ono, and L. Rolen, *Harmonic Maass Forms and Mock Modular Forms: Theory and Applications*, Colloquium publications, Amer. Math. Soc. (2017), to appear.

[10] K. Bringmann and K. Ono, *The $f(q)$ mock theta function conjecture and partition ranks*, Invent. Math. **165** (2006), 243–266.

[11] ______, *Arithmetic properties of coefficients of half-integral weight harmonic Maass forms*, Math. Ann. **337** (2007), 591–612.

[12] ______, *Dyson's ranks and Maass forms*, Ann. Math. **171** (2010), 419–449.

[13] J. H. Bruinier and J. Funke, *On two geometric theta lifts*, Duke Math. J. **1** (2004), no. 125, 45–90.

[14] ______, *Traces of CM values of modular functions*, J. Reine Angew. Math. **594** (2006), 1–33.

[15] J. H. Bruinier and Y. Li, *Heegner divisors in generalized Jacobians and traces of singular moduli*, Algebra Number Theory **10** (2016), no. 6, 1277–1300.

[16] J. H. Bruinier and K. Ono, *Heegner divisors, L-functions, and harmonic weak Maass forms*, Ann. Math. **172** (2010), 2135-2181.

[17] S. H. Carnahan, *Generalized Moonshine IV: Monstrous Lie Algebras*, preprint, available at `https://arxiv.org/abs/1208.6254`, 2012.

[18] M. C. N. Cheng and J. F. R. Duncan, *On Rademacher Sums, the Largest Mathieu Group, and the Holographic Modularity of Moonshine*, Commun. Number Theory Physics **6** (3) (2012), 697–758.

[19] ______, *Rademacher Sums and Rademacher Series*, in W. Kohnen (ed.) and R. Weissauer (ed.) *Conformal Field Theory, Automorphic Forms and Related Topics: CFT, Heidelberg, September 19-23, 2011*, Springer-Verlag, 2014, 143–182.

[20] ______, *Optimal Mock Jacobi Theta Functions*, preprint, available at `https://arxiv.org/abs/1605.04480`, 2016.

[21] M. Cheng, J. Duncan, and J. Harvey, *Umbral Moonshine*, Commun. Number Theory Phys. **8** (2014), no. 2, 101–242.

[22] ______, *Umbral Moonshine and the Niemeier Lattices*, Res. Math. Sci. **1** (2014), Art. 3, 81 pp.

[23] ———, *Weight One Jacobi Forms and Umbral Moonshine*, preprint, 2017.

[24] J. H. Conway and S. P. Norton, *Monstrous Moonshine*, Bull. London Math. Soc. **11** (1979), 308–339.

[25] J. E. Cremonia, *Computing the degree of the modular parameterization of a modular elliptic curve*, Math. Comp. **64** (1995), 1235-1250.

[26] A. Dabholkar, S. Murthy, D. Zagier, *Quantum Black Holes, Wall Crossing, and Mock Modular Forms*, to appear in Cambridge Monographs in Mathematical Physics, available at `http://arxiv.org/abs/1208.4074`.

[27] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Invent. Math. **92** (1988), 73–90.

[28] W. Duke and R. Schulze-Pillot, *Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids*, Invent. Math. **99** (1990), 49–57.

[29] J. F. R. Duncan, *Moonshine for Rudvalis's sporadic group I*, arXiv:math/0609449.

[30] J. F. R. Duncan, *Moonshine for Rudvalis's sporadic group II*, arXiv:math/0611355.

[31] J. F. R. Duncan and I. B. Frenkel, *Rademacher sums, moonshine, and gravity*, Commun. Number Theory Phys. **5** (2011), no. 4, 1–128.

[32] J. F. R. Duncan, M. J. Griffin, and K. Ono, *Proof of the Umbral Moonshine Conjecture*, Res. Math. Sci. **2** (2015), Art. 26, 47 pp.

[33] J. F. R. Duncan, M. J. Griffin, and K.Ono, *Moonshine*, Res. Math. Sci. **2** (2015), Art. 11, 57 pp.

[34] T. Eguchi, H. Ooguri, and Y. Tachikawa, *Notes on the K3 Surface and the Mathieu Group M_{24}*, Experiment. Math. **20** (2011), no. 1, 91–96.

[35] D. Ford, J. McKay, and S. P. Norton, *More on replicable functions*, Commun. Algebra **22** (1994), no. 13, 5175–5193.

[36] I. Frenkel, J. Lepowsky, and A. Meurman, *A natural representation of the Fischer-Griess Monster with the modular function J as character*, Proc. Nat. Acad. Sci. U.S.A. **81** (1984), no. 10, Phys. Sci., 3256–3260.

[37] ———, *A moonshine module for the Monster*, Vertex operators in mathematics and physics (Berkeley, Calif., 1983), Math. Sci. Res. Inst. Publ., vol. 3, Springer, New York, 1985, pp. 231–273.

[38] ———, *Vertex operator algebras and the Monster*, Pure and Applied Mathematics, vol. 134, Academic Press Inc., Boston, MA, 1988.

[39] T. Gannon, *Monstrous moonshine: the first twenty-five years*, Bull. London Math. Soc. **38** (2006), no. 1, 1–33.

[40] ———, *Much ado about Mathieu*, Adv. Math. **301** (2016), 322–358.

[41] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.8;* 2016, `http://www.gap-system.org`.

[42] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, in Num- ber theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illi- nois Univ., Carbondale, Ill., 1979), M. B. Nathanson, ed., Lect. Notes in Math. **751**, Springer, Berlin, 1979, 108–118.

[43] R. L. Griess Jr., *The friendly giant*, Invent. Math. **69** (1982), no. 1, 1–102.

[44] M. J. Griffin and M. H. Mertens, *A proof of the Thompson Moonshine Conjecture*, Res. Math. Sci. **3** (2016), Art. 36, 32 pp.

[45] B. Gross, *The classes of singular moduli in the generalized Jacobian*, Geometry and arithmetic (Ed. C. Faber et. al.), European Math. Soc., Zürich (2012), 137–141.

[46] B. Gross, W. Kohnen, and D. Zagier, *Heegner Points and Derivatives of L-series. II*, Math. Ann. **278** (1987), 497–562.

[47] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **85** (1986), 225–320.

[48] J. A. Harvey and B. C. Rayhaun, *Traces of Singular Moduli and Moonshine for the Thompson Group*, Commun. Number Theory Phys. **10** (2016), no. 1, 23-62.

[49] F. Hirzebruch and D. Zagier, *Intersection Numbers of Curves on Hilbert Modular Surfaces and Modular Forms of Nebentypus*, Invent. Math. **36** (1976), 57–113.

[50] Hua L. K., *Introduction to Number Theory*, Springer-Verlag Berlin Heidelberg New York, 1982.

[51] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Invent. Math. **87** (1987), 385–401.
[52] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Colloquium Publications **53**, Amer. Math. Soc., Providence, RI., 2004.
[53] W. Kohnen, *Fourier Coefficients of Modular Forms of Half-Integral Weight*, Math. Ann. **271** (1985), 237–268.
[54] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $X(E,\mathbb{Q})$ for a class of Weil curves*, Math. USSR Izv. **32** (1989), 523–541.
[55] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, `http://www.lmfdb.org`, 2016, [Online, accessed 31 Jan. 2017].
[56] M. Manickam, B. Ramakrishnan, and T. C. Vasudevan, *On Shintani correspondence*, Proc. Indian Acad. Sci. (Math Sci.) **99** (1989), 235–247.
[57] A. Miller and A. Pixton, *Arithmetic traces of non-holomorphic modular invariants*, Int. J. Number Theory **6** (2010), 69–87.
[58] S. P. Norton, *Generalized Moonshine*, Proc. Symp. Pure Math **47** (1987), 208–209.
[59] A. P. Ogg, *Automorphismes de courbes modulaires*, Séminaire Delange-PisotPoitou (16e année: 1974/75), Théorie des nombres, Fasc. 1, Exp. No. 7, Secrétariat Mathématique, Paris, 1975, p. 8.
[60] M. E. O'Nan, *Some evidence for the existence of a new simple group*, Proc. London Math. Soc. **32** (1976), 421-479.
[61] K. Ono, *Unearthing the visions of a master: harmonic Maass forms and number theory*, Current Developments in Mathematics **2008** (2009), 347–454.
[62] L. Queen, *Modular functions arising from some finite groups*, Math. Comp. **37** (1981), no. 156, 547–580.
[63] H. Rademacher, *The Fourier coefficients of the modular invariant $J(\tau)$*, Amer. J. Math. **60** (1938), 501–512.
[64] J. Rouse and J. J. Webb, *Spaces of modular forms spanned by eta-quotients*, Adv. Math. **272** (2015), 200–224.
[65] J.-P. Serre, *Proprietés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
[66] J-P. Serre and H. M. Stark, *Modular Forms of Weight 1/2*, Modular Functions of One Variable VI (J.-P. Serre and D. B. Zagier, eds.), Lecture Notes in Mathematics, vol. 627, Springer Berlin Heidelberg, 1977, 27–67.
[67] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, New York, 2009.
[68] C. Skinner, *Multiplicative reduction and the cyclotomic main conjecture for* GL_2, Pacific J. Math. **283** (2016), no. 1, 171–200.
[69] C. Skinner and E. Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195** (2014), no. 1, 1–277.
[70] J. Sturm, *On the congruence of modular forms*, Number Theory (New York, 1984-1985), Springer Lect. Notes. Math. **1240**, (1987), Springer, Berlin, 275-280.
[71] J. G. Thompson, *Finite groups and modular functions*, Bull. London Math. Soc. **11** (1979), no. 3, 347–351.
[72] ———, *Some numerology between the Fischer-Griess Monster and the elliptic modular function*, Bull. London Math. Soc. **11** (1979), no. 3, 352–353.
[73] M. Ueda, *The decomposition of the spaces of cusp forms of half-integral weight and trace formula of Hecke operators*, J. Math. Kyoto Univ. **28** (1988), 505–555.
[74] M. Ueda and S. Yamana, *On newforms for Kohnen plus spaces*, Math. Z. **264** (2010), 1–13.
[75] R. A. Wilson, *Is J_1 a subgroup of the Monster?*, Bull. LMS 18 (1986), 349–350.
[76] D. Zagier, *Nombres de classes et formes modulaires de poids* $3/2$, C. R. Acad. Sci. Paris Sér. A-B **281** (1975), no. 21, Ai, A883–A886.
[77] ———, *Zetafunktionen und quadratische Körper - Eine Einführung in die höhere Zahlentheorie*, Springer-Verlag Berlin Heidelberg New York, 1981.
[78] ———, *Modular parameterizations of elliptic curves*, Canadian Math. Bull. **28** (1985), 372-384.

[79] ———, *Traces of singular moduli*, in "Motives, Polylogarithms and Hodge Theory" (Eds. F. Bogomolov, L. Katzarkov), Lecture Series **3**, International Press, Somerville (2002), 209–244.
[80] ———, *Ramanujan's mock theta functions and their applications [d'après Zwegers and Bringmann-Ono]*, Séminaire Bourbaki, 60ème année, 2006-2007, no. 986.
[81] S. Zwegers, *Mock Theta Functions*, Ph.D. thesis, Universiteit Utrecht, 2002.

Department of Mathematics and Computer Science, Emory University, 400 Dowman Drive, Atlanta, GA 30322
E-mail address: john.duncan@emory.edu

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn
E-mail address: mhmertens@mpim-bonn.mpg.de

Department of Mathematics and Computer Science, Emory University, 400 Dowman Drive, Atlanta, GA 30322
E-mail address: ono@mathcs.emory.edu