

# $p$ -Adic Properties of Hauptmoduln with Applications to Moonshine

Ryan C. CHEN, Samuel MARKS and Matthew TYLER

Department of Mathematics, Princeton University, Princeton, NJ 08544, USA

E-mail: [rcchen@princeton.edu](mailto:rcchen@princeton.edu), [spmarks@princeton.edu](mailto:spmarks@princeton.edu), [mttyler@princeton.edu](mailto:mttyler@princeton.edu)

Received September 19, 2018, in final form April 10, 2019; Published online April 29, 2019

<https://doi.org/10.3842/SIGMA.2019.033>

**Abstract.** The theory of monstrous moonshine asserts that the coefficients of Hauptmoduln, including the  $j$ -function, coincide precisely with the graded characters of the monster module, an infinite-dimensional graded representation of the monster group. On the other hand, Lehner and Atkin proved that the coefficients of the  $j$ -function satisfy congruences modulo  $p^n$  for  $p \in \{2, 3, 5, 7, 11\}$ , which led to the theory of  $p$ -adic modular forms. We combine these two aspects of the  $j$ -function to give a general theory of congruences modulo powers of primes satisfied by the Hauptmoduln appearing in monstrous moonshine. We prove that many of these Hauptmoduln satisfy such congruences, and we exhibit a relationship between these congruences and the group structure of the monster. We also find a distinguished class of subgroups of the monster with graded characters satisfying such congruences.

*Key words:* modular forms congruences;  $p$ -adic modular forms; moonshine

*2010 Mathematics Subject Classification:* 11F11; 11F22; 11F33

## 1 Introduction and statements of results

The theory of monstrous moonshine arose from the remarkable observation of McKay and Thompson [41] that

$$196884 = 1 + 196883$$

and its generalizations, including

$$21493760 = 1 + 196883 + 21296876,$$

$$864299970 = 2 \times 1 + 2 \times 196883 + 21296876 + 842609326,$$

$$20245856256 = 2 \times 1 + 3 \times 196883 + 2 \times 21296876 + 842609326 + 19360062527.$$

Here, the left-hand sides of the equations are the coefficients of the *normalized modular  $j$ -function*

$$J(\tau) = j(\tau) - 744 = q^{-1} + 196884q + 21493760q^2 + \dots, \quad \text{where } q = e^{2\pi i\tau},$$

and the right-hand sides are simple sums involving the dimensions of the irreducible representations of the monster group  $\mathbb{M}$ :

$$1, 196883, 21296876, 842609326, 19360062527, \dots$$

Thompson conjectured [40] that these identities could be explained by the existence of an infinite-dimensional graded *monster module*

$$V^{\natural} = \bigoplus_{n=-1}^{\infty} V_n^{\natural}$$

such that the graded dimension is given by  $J$ . More generally, the graded-trace functions

$$\mathcal{T}_g(\tau) = \sum_{n=-1}^{\infty} \text{Tr}(g|V_n^{\natural})q^n$$

for the action of  $\mathbb{M}$  on  $V^{\natural}$  are known as the *McKay–Thompson series* and depend only on the conjugacy class of  $g \in \mathbb{M}$ . As part of their famous monstrous moonshine conjectures, Conway and Norton computed for each monster conjugacy class  $g$  a genus zero group  $\Gamma_g \leq \text{GL}_2^+(\mathbb{R})$  on which they conjectured  $\mathcal{T}_g$  was a *normalized Hauptmodul* [10]. That is, each  $\mathcal{T}_g$  was conjectured to be the unique generator  $\mathcal{T}_{\Gamma_g}$  of the function field of the genus zero curve  $\Gamma_g \backslash \mathbb{H}^*$  having  $q$ -expansion of the form  $q^{-1} + O(q)$  at  $\infty$ . Since all of the Hauptmoduln appearing in this paper will be normalized (meaning that they are bounded away from  $\infty$  and have  $q$ -expansion  $q^{-1} + O(q)$  at  $\infty$ ), we will henceforth omit the word “normalized” and refer to such functions simply as *Hauptmoduln*. Frenkel–Lepowsky–Meurman [18, 19] constructed  $V^{\natural}$  with the correct graded dimensions, and Borcherds [4] proved that the McKay–Thompson series were Hauptmoduln for the  $\Gamma_g$  given by Conway–Norton. After the proof of monstrous moonshine, different incarnations of moonshine were shown for other finite groups, such as the largest Mathieu group  $M_{24}$  [20], and later the other 22 groups appearing in umbral moonshine [14]. There is also a notion of generalized moonshine, conjectured by Norton [33] and recently proved by Carnahan [8].

Thirty years before the observation of McKay and Thompson, Lehner [31, 32] and Atkin [2] proved that the Fourier expansion of  $J(\tau) = q^{-1} + \sum c(n)q^n$  satisfies the following congruences for all positive  $\alpha$ :

$$\begin{aligned} c(2^\alpha n) &\equiv 0 \pmod{2^{3\alpha+8}}, \\ c(3^\alpha n) &\equiv 0 \pmod{3^{2\alpha+3}}, \\ c(5^\alpha n) &\equiv 0 \pmod{5^{\alpha+1}}, \\ c(7^\alpha n) &\equiv 0 \pmod{7^\alpha}, \\ c(11^\alpha n) &\equiv 0 \pmod{11^\alpha}. \end{aligned} \tag{1.1}$$

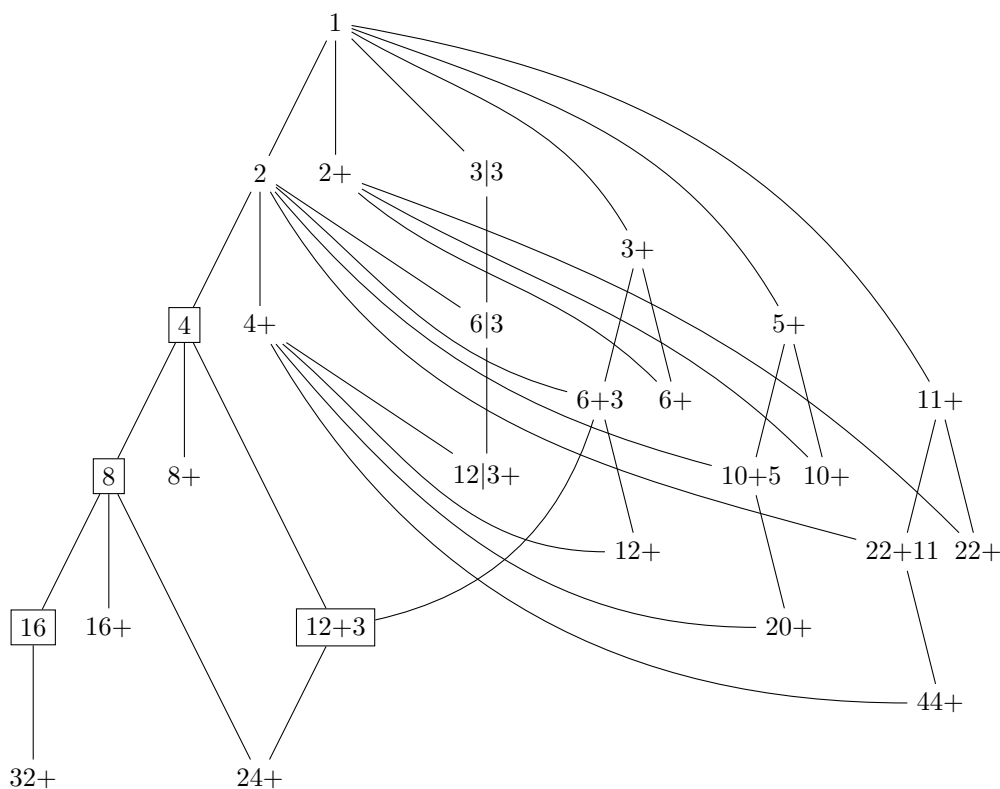
Viewed another way, these identities state that  $J|U_p^n$  uniformly converges to zero  $p$ -adically as  $n \rightarrow \infty$ , where  $U_p$  is the operator defined on  $q$ -expansions by

$$\left( \sum a(n)q^n \right) |U_p = \sum a(pn)q^n.$$

Such congruences led Serre, Katz, and others to develop a robust and fruitful theory of  $p$ -adic modular forms [7, 22, 28, 29, 37].

Given the deep connections between  $J$  and the monster, one might wonder whether these  $p$ -adic properties of  $J$  are special cases of a more general  $p$ -adic phenomenon taking place among the Hauptmoduln appearing in monstrous moonshine. To make this more precise, given a prime  $p$  and a modular function  $f$ , we say that  $f$  is  *$p$ -adically annihilated* if the  $q$ -series  $f|U_p^n$  uniformly converges to 0 in the  $p$ -adic limit as  $n \rightarrow \infty$ . Given that  $J$  is  $p$ -adically annihilated for  $p \in \{2, 3, 5, 7, 11\}$ , we can then ask if other Hauptmoduln appearing in monstrous moonshine are as well.

There is some literature studying coefficient congruences of a related nature. The papers [1, 26] discuss Hauptmoduln on  $\Gamma_0(N)$ , and [40] discusses other coefficient congruences involving



**Figure 1.1.** Conjugacy classes with 2-adically annihilated Hauptmoduln and their power maps.

Hauptmoduln. However, there has not been a systematic study of  $p$ -adic annihilation for all of the monstrous moonshine Hauptmoduln.

Our first main result is that  $p$ -adic annihilation is actually quite common among the Hauptmoduln of monstrous moonshine. In fact, out of the 171 Hauptmoduln in monstrous moonshine, we will show that 97 have  $p$ -adic annihilation for some prime  $p$ .

**Theorem 1.1.** *For primes  $p \in \{2, 3, 5, 7, 11\}$ , the Hauptmoduln  $\mathcal{T}$  corresponding to the genus zero groups of monstrous moonshine appearing in Table 4.1 are  $p$ -adically annihilated.*

We further conjecture that Table 4.1 gives *all* the Hauptmoduln appearing in monstrous moonshine that are  $p$ -adically annihilated for any prime  $p$  (see Conjecture 4.2).

Once Theorem 1.1 has established a class of Hauptmoduln coming from monstrous moonshine with  $p$ -adic annihilation, we may next ask whether the structure of the monster group informs  $p$ -adic properties of the Hauptmoduln. Specifically, we are interested in relating the *power maps*  $g \mapsto g^m$  of the monster (or equivalently, the corresponding maps of conjugacy classes) to  $p$ -adic annihilation of Hauptmoduln.

**Theorem 1.2.** *Let  $\mathcal{T}_g$  be the Hauptmodul of a group appearing in Table 4.1, so that  $\mathcal{T}_g$  is  $p$ -adically annihilated by Theorem 1.1. Outside of the exceptions discussed in Section 4.4, we also have that  $\mathcal{T}_{g^m}$  is  $p$ -adically annihilated for any  $m \in \mathbb{N}$ .*

Although Theorem 1.2 follows from Theorem 1.1, we will prove the two theorems in tandem, relying on the structure provided by Theorem 1.2 to make Theorem 1.1 easier to prove. As an illustration of Theorem 1.2, see Fig. 1.1, which shows conjugacy classes with Hauptmoduln that are 2-adically annihilated and the power maps between them. For a full explanation of the notation used in this figure, and the corresponding figures for  $p = 3, 5, 7, 11$ , see Appendix B.

Finally, we consider which finite groups have infinite-dimensional representations with similar  $p$ -adic properties. We define a *moonshine module* for a finite group  $G$  to be a graded  $G$ -module  $V = \bigoplus_{n=-1}^{\infty} V_n$  such that for each  $g \in G$  the graded trace  $\mathcal{T}_g = \sum \text{Tr}(g|V_n)q^n$  associated to the action of  $g$  on  $V$  is the Hauptmodul of an order  $\text{ord}(g)$  conjugacy class of the monster. We also require that the power maps of  $G$  interact with the Hauptmoduln in a way that mimics what occurs in monstrous moonshine; see Section 5 for the precise condition. For an irreducible character  $\chi$  of  $G$ , we write  $m_\chi(n)$  for the multiplicity of  $\chi$  appearing in the character of  $G$  acting on  $V_n$ , and define the *multiplicity generating function*

$$\mathcal{M}_\chi(\tau) = \sum_{n=-1}^{\infty} m_\chi(n)q^n.$$

These series  $\mathcal{M}_\chi$  were perhaps first studied in [23]. We say that a moonshine module  $V$  for  $G$  is a  *$p$ -adic moonshine module* if  $\mathcal{M}_\chi$  is  $p$ -adically annihilated for each irreducible character  $\chi$ . We may then ask various questions about finite groups with  $p$ -adic moonshine modules, such as the number of such groups and which primes may divide their orders. In Section 5 we address these questions and give examples of groups with  $p$ -adic moonshine modules. In particular, we find that the groups in Table 1.2 have  $p$ -adic moonshine for the listed  $p$  in a slightly more general sense explained in Section 5.3. These groups arise as the centralizers of certain commuting pairs of elements of the monster in the conjugacy class  $pA$ . For other instances of moonshine modules for centralizers of elements of the class  $pA$ , see Ryba's modular moonshine conjectures [35], which were proved by Borcherds and Ryba [5, 6].

$p$	2	3	5	7	11
$C(pA^2)$	$2^2 \cdot {}^2E_6(2)$	$3^2 \times O_8^+(3)$	$5^2 \times U_3(5)$	$7^2 \times L_2(7)$	$11^2$
$\#C(pA^2)$	$2^{38} \cdot 3^9 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$2^{12} \cdot 3^{14} \cdot 5^2 \cdot 7 \cdot 13$	$2^4 \cdot 3^2 \cdot 5^5 \cdot 7$	$2^3 \cdot 3 \cdot 7^3$	$11^2$

**Table 1.2.** Subgroups of the monster with weakly  $p$ -adic moonshine.

Before proceeding, we outline the structure of this paper. We begin in Section 2 by proving technical lemmas that will be useful later in the paper. In Section 3, we extend Serre's theory of  $p$ -adic modular forms such that it becomes applicable to the groups appearing in monstrous moonshine, and we begin to see  $p$ -adic properties of Hauptmoduln. In Section 4, we prove Theorems 1.1 and 1.2 using both the theory of Section 3 and the interplay between power maps and  $p$ -adic properties. We conclude in Section 5 by considering finite groups with  $p$ -adic moonshine modules, and showing that only finitely many such groups exist. We also discuss examples of groups with  $p$ -adic moonshine, including those in Table 1.2.

## 2 Preliminaries

In this section, we collect technical details and definitions that will be used later. We first describe the types of groups  $\Gamma$  whose Hauptmoduln will be studied. We then discuss various properties of operators on spaces of modular forms, most importantly the  $U_p$  operator and the Atkin–Lehner involutions. We also give descriptions of which cusps a Hauptmodul may have poles at once  $U_p$  is applied to it, and we give a modular form  $g$  with zeros at all such cusps. Finally, we discuss the trace of a modular form, which transforms modular forms on some  $\Gamma$  into modular forms on some  $\Gamma' \geq \Gamma$ . These facts will ultimately be used to interpret Hauptmoduln as  $p$ -adic modular forms in Section 3.

### 2.1 $n|h$ -type groups

Monstrous moonshine associates to each  $g \in \mathbb{M}$  a Hauptmodul  $\mathcal{T}_g$  for some genus zero group  $\Gamma_g \leq \mathrm{GL}_2(\mathbb{R})^+$ . This means that  $\Gamma_g \backslash \mathbb{H}^*$  is a genus zero curve and that  $\mathcal{T}_g$  is a generator for the function field such that  $\mathcal{T}_g$  is bounded away from the cusp  $\infty$ ; moreover the  $q$ -expansion of  $\mathcal{T}_g$  at infinity begins  $\mathcal{T}_g = q^{-1} + O(q)$ . Conway and Norton described the groups  $\Gamma_g$  in [10], all of which take on a particular form which we reproduce here.

First we describe the normalizer of  $\Gamma_0(N)$  in  $\mathrm{PSL}_2(\mathbb{R})$ . Let  $h$  be the largest integer such that  $h^2|N$  and  $h|24$ , and set  $n = N/h$ . The normalizer of  $\Gamma_0(N)$  is given by  $\bigcup_{e||n/h} w_e$  where  $w_e$  is the set of all matrices  $A = \begin{pmatrix} ae & b/h \\ cn & de \end{pmatrix}$  such that  $a, b, c, d \in \mathbb{Z}$  and  $\det A = e$ . Here the notation  $x|y$  means that  $x$  exactly divides  $y$ , i.e., that  $x|y$  and  $\gcd(x, y/x) = 1$ . Given integers  $e_1, e_2$  we set  $e_1 * e_2 = \frac{e_1 e_2}{\gcd(e_1, e_2)^2}$ , and under  $*$  the set of exact divisors of any integer  $N$  forms the abelian group  $(\mathbb{Z}/2\mathbb{Z})^n$  where  $n$  is the number of primes dividing  $N$ .

More generally, a class of subgroups called  $n|h$ -type groups is defined as follows. Let  $n$  be any positive integer and let  $h|\gcd(n, 24)$ . Set  $N = nh$  and  $w_e$  as above, for  $e||n/h$ . We define the group  $\Gamma_0(n|h) = w_1$ . We will often abuse notation and write  $w_e$  for any element of  $w_e$ , and we see that  $w_{e_1} w_{e_2} = w_{e_1 * e_2}$ . Since  $h|24$  we have that  $m^2 \equiv 1 \pmod{h}$  for all  $m$  coprime to  $h$ . For a subgroup  $\{1, e_1, \dots, e_n\}$  of the group of exact divisors of  $n/h$ , we then define

$$\Gamma_0(n|h)+e_1, e_2, \dots, e_n = \langle \Gamma_0(n|h), w_{e_1}, w_{e_2}, \dots, w_{e_n} \rangle = w_1 \cup w_{e_1} \cup w_{e_2} \cup \dots \cup w_{e_n}.$$

A group of this form is called an  $n|h$ -type group.

Setting  $N = nh$ , the group  $\Gamma_0(n|h)+e_1, \dots, e_n$  normalizes both  $\Gamma_0(n|h)$  and  $\Gamma_0(N)$ , and the  $w_{e_i}$  are cosets of  $\Gamma_0(n|h)$ . When  $h = 1$  we have  $\Gamma_0(n|1) = \Gamma_0(N)$  and we denote the matrix

$$w_e = \begin{pmatrix} ae & b \\ cN & de \end{pmatrix}$$

by  $W_e$ . The matrices  $W_e$  for  $e||N$  are called *Atkin–Lehner involutions*. Given an Atkin–Lehner involution  $W_E$  on  $\Gamma_0(N)$ , we can interpret this as an element of  $\Gamma_0(n|h)$  via

$$W_E = \begin{pmatrix} aE & b \\ cN & dE \end{pmatrix} = \begin{pmatrix} aE/h_E & b/h_E \\ cN/h_E & dE/h_E \end{pmatrix} = w_e,$$

where  $h_E$  is the largest divisor of  $h$  with  $h_E^2|E$  and  $e = E/h_E^2$ . In fact, setting

$$\mathrm{AL}(\Gamma) = \{e||nh : W_e \in \Gamma \text{ and every prime dividing } e \text{ also divides } n/h\}$$

we have that this association gives a bijection

$$\mathrm{AL}(\Gamma) \longleftrightarrow \{e : w_e \subset \Gamma\}.$$

For example, letting  $\Gamma = \Gamma_0(8|2)+4$  we have

$$\mathrm{AL}(\Gamma) = \{1, 16\} \longleftrightarrow \{1, 4\} = \{e : w_e \subset \Gamma\}.$$

When dealing with  $n|h$ -type groups, it is standard to simplify notation in the following ways. When  $h = 1$ , we simply omit the  $|h$ , so that  $\Gamma_0(n|1) = \Gamma_0(n)$ , and when all  $e||n/h$  are included in a group, we simply write  $\Gamma_0(n|h)+$  so that  $\Gamma_0(8|2)+ = \Gamma_0(8|2)+4$ . We will also sometimes use the symbol  $n|h+e, f, \dots$  to represent the group  $\Gamma_0(n|h)+e, f, \dots$  in order to save space, particularly in tables, so we might write  $8|2+$  instead of  $\Gamma_0(8|2)+$ .

The  $n|h$ -type groups appear in monstrous moonshine as *eigengroups* of the Hauptmoduln. That is, the Hauptmodul  $\mathcal{T}$  has an associated group  $\Gamma_0(n|h)+e, \dots$  such that for all  $A$  in this group,  $\mathcal{T}(A\tau) = \mu\mathcal{T}(\tau)$  for some  $h^{\mathrm{th}}$  root of unity  $\mu$ . Conway–Norton [10] conjectured the following rule for computing the eigenvalue  $\lambda$  corresponding to an element of  $\Gamma_0(n|h)+e, \dots$ :

- (i)  $\lambda = 1$  for any element of  $\Gamma_0(N)$ ,
- (ii)  $\lambda = 1$  for all  $W_e$  with  $e \in \text{AL}(\Gamma)$ ,
- (iii)  $\lambda = e^{-2\pi i/h}$  for the element  $x = \begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix}$ ,
- (iv)  $\lambda = e^{\pm 2\pi i/h}$  for the element  $y = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$  where the sign is  $+$  if and only if  $\tau \mapsto \frac{-1}{N\tau}$  is in  $\Gamma_0(n|h)+e, \dots$

This rule's well-definedness and correctness follow from [17] and the correctness of the monstrous moonshine conjectures, respectively.

Since the cosets  $x$  and  $y$  generate  $\Gamma_0(n|h)$ , we have  $\Gamma = \langle x, y, W_e : e \in \text{AL}(\Gamma) \rangle$  for any  $n|h$ -type group  $\Gamma$ . Hence Conway–Norton's rule uniquely determines a map  $\lambda: \Gamma \rightarrow \mu_h$  where  $\mu_h$  denotes the group of  $h^{\text{th}}$  roots of unity. We always use  $\lambda$  to denote this map.

More generally, let  $\Gamma$  be an  $n|h$ -type group. An *eigenvalue map* is a homomorphism  $\eta: \Gamma \rightarrow \mu_{2h}$  such that  $\Gamma_0(nh) \subset \ker \eta$ . Then we define

$$\Gamma_\eta = \ker \eta.$$

When  $\lambda$  is the map given by Conway–Norton's rule, we have that  $\Gamma_\lambda$  is an index  $h$  subgroup of  $\Gamma$  called the *fixing group* of  $\Gamma$ . However, Conway–Norton's rule does not always give a well-defined map, so  $\Gamma_\lambda$  does not exist for every  $n|h$ -type group  $\Gamma$ ; for example  $\Gamma_\lambda$  doesn't exist when  $\Gamma = \Gamma_0(21|3)$ . Ferenbaugh [17, Theorem 2.8] classified the groups  $\Gamma$  for which Conway–Norton's rule is consistent, and we call such  $\Gamma$  *admissible*. There are 213 admissible  $n|h$ -type groups giving genus zero groups, including all 171 groups appearing in monstrous moonshine. Ferenbaugh also determined the structure of the quotient  $\Gamma/\Gamma_0(nh)$ , and therefore also the structure of  $\Gamma_\lambda/\Gamma_0(nh)$ . In 174 cases, including the groups of monstrous moonshine, the latter quotient group has exponent 2; the remaining 3 groups are known as the “ghosts”. For further discussion of which  $n|h$ -type groups appear in monstrous moonshine, see [11].

In the next section we study modular forms on  $n|h$ -type groups with given eigenvalue maps, and the action of the  $U_p$  operator on such spaces of modular forms.

## 2.2 Action of $U_p$ on Hauptmoduln

Given an  $n|h$ -type group  $\Gamma$  with eigenvalue map  $\eta: \Gamma \rightarrow \mu_{2h}$ , we say a weight  $k$  weakly holomorphic modular form on  $\Gamma_0(nh)$  is *on  $\Gamma$  with eigenvalue map  $\eta$*  or *on  $(\Gamma, \eta)$*  if

$$f|_k \gamma = \eta(\gamma) f \quad \text{for all } \gamma \in \Gamma,$$

where the weight  $k$  slash operator is defined by (2.1) below. By a *weakly holomorphic modular form* we mean a meromorphic modular form whose poles are supported on the cusps; on the other hand a *modular form* is assumed to be holomorphic everywhere. We write  $M_k(\Gamma, \eta)$  for the space of weight  $k$  modular forms on  $\Gamma$  with eigenvalue map  $\eta$ . Similarly, we denote the space of weight  $k$  modular forms on  $\Gamma_0(nh)$  invariant under all  $\gamma \in \Gamma_\eta$  by  $M_k(\Gamma_\eta)$ . Throughout, all our weights will be integers.

Fix a prime  $p$ . In this section, we study  $U_p$  applied to Hauptmoduln  $\mathcal{T}$ , and more generally weakly holomorphic modular forms on  $\Gamma_\eta$  or on  $\Gamma$  with eigenvalue map  $\eta$ . For our results to extend to  $n|h$ -type groups, the results of this section will be stated in the necessary general language. However the reader looking to use these results for modular forms on  $\Gamma_0(N)+e, \dots$  should remember that this corresponds to taking  $h = 1$  and ignoring eigenvalue maps in the following results.

Recall that the weight  $k$  slash operator  $|_k \gamma$  for  $\gamma \in \text{GL}_2^+(\mathbb{R})$  is defined by

$$(f|_k \gamma)(\tau) = (\det \gamma)^{k/2} (c\tau + d)^{-k} f(\gamma\tau). \tag{2.1}$$

If  $f$  is on  $\mathrm{SL}_2(\mathbb{Z})$  then for  $N \in \mathbb{N}$ , we have  $f(N\tau)$  on  $\Gamma_0(N)$ , and for  $d|N$  and  $e||N$ ,

$$f(d\tau)|_k W_e = \left( \frac{d * e}{d} \right)^{k/2} f((d * e)\tau). \quad (2.2)$$

In terms of the slash operator,  $U_p$  is defined on weight  $k$  modular forms by

$$f|U_p = p^{k/2-1} \sum_{\mu=0}^{p-1} f|_k S_\mu = \frac{1}{p} \sum_{\mu=0}^{p-1} f(S_\mu\tau), \quad (2.3)$$

where  $S_\mu = \begin{pmatrix} 1 & \mu \\ 0 & p \end{pmatrix}$ . This operator is independent of  $k$  and acts on Fourier expansions by

$$\left( \sum a(n)q^n \right) |U_p = \sum a(pn)q^n.$$

We first recall some basic facts about the  $U_p$  operator (see [3, Section 2]).

**Lemma 2.1.** *Let  $f$  be a weight  $k$  meromorphic modular form on  $\Gamma_0(p^\alpha N)$  where  $p \nmid N$ .*

- (a) *If  $e||N$  then  $f|U_p|_k W_e = f|_k W_e|U_p$ .*
- (b)  *$f|U_p$  is modular on  $\Gamma_0(p^\beta N)$  where  $\beta = \max\{1, \alpha - 1\}$ .*

The following lemma extends these facts from  $\Gamma_0(N)$  to  $n|h$ -type groups.

**Lemma 2.2.** *Let  $p \nmid nh$  be prime, and let  $f$  be a weight  $k$  meromorphic modular form on a  $p^\alpha n|h$ -type group  $\Gamma$  with eigenvalue map  $\eta$ .*

- (a) *Let*

$$x = \begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 1 & 0 \\ p^{\alpha n} & 1 \end{pmatrix}$$

*be the matrices of Section 2.1. Then*

$$f|U_p|_k x^p = f|_k x|U_p \quad \text{and} \quad f|U_p|_k y^p = f|_k y|U_p.$$

- (b) *Let  $\Gamma'$  be the  $p^\beta n|h$ -type group such that  $\beta = \max\{1, \alpha - 1\}$  and  $e \in \mathrm{AL}(\Gamma')$  if and only if  $e \in \mathrm{AL}(\Gamma)$  and  $p \nmid e$ . Let  $\eta'$  be an eigenvalue map on  $\Gamma'$  such that*

$$\eta'(x^p) = \eta(x), \quad \eta'(y^p) = \eta(y), \quad \eta'(W_e) = \eta(W_e) \quad \text{for } e \in \mathrm{AL}(\Gamma').$$

*Then  $f|U_p$  is on  $\Gamma'$  with eigenvalue map  $\eta'$ .*

**Proof.** For  $0 \leq \mu \leq p - 1$ , let  $S_\mu = \begin{pmatrix} 1 & \mu \\ 0 & p \end{pmatrix}$  denote the matrix appearing in the definition (2.3) of  $U_p$ . The first identity of part (a) follows from the equation  $S_\mu x^p = x S_\mu$ . The second identity follows from the equation

$$S_\mu y^p = \begin{pmatrix} * & * \\ p^{\alpha n}(-1 + p^2 + p^{\alpha+1}n\mu) & * \end{pmatrix} y S_\mu, \quad (2.4)$$

where each  $*$  is an integer such that the matrix has determinant 1. Since  $p \nmid h$ , we have that  $p^2 \equiv 1 \pmod{h}$  (since  $h$  is a divisor of 24), so the matrix appearing in (2.4) is in  $\Gamma_0(p^\alpha nh)$  and therefore fixes  $f$ .

For part (b), note that since  $p \nmid h$  and  $\beta \leq \alpha + 1$ , the matrices  $x^p$  and  $y^p$  generate  $\Gamma_0(p^\beta n|h)$ . Thus part (b) follows from part (a) and Lemma 2.1. ■



Let  $\sigma_a: \mu \mapsto \mu^a$  be an endomorphism of  $\mu_{2h}$ . We set  $\eta^{\sigma_a} = \sigma_a \circ \eta$ . The preceding lemma says that if  $\Gamma$  is an  $pn|h$ -type group with  $p \nmid nh$  then  $U_p$  is a map  $M_k(\Gamma, \eta) \rightarrow M_k(\Gamma, \eta^{\sigma_p})$ .

Analogous to the decomposition  $M_k(\Gamma_1(N)) = \bigoplus_{\chi} M_k(\Gamma_0(N), \chi)$  over mod  $N$  Dirichlet characters  $\chi$ , we have the following decomposition of  $M_k(\Gamma_\eta)$ .

**Lemma 2.3.** *Let  $\Gamma$  be an  $n|h$ -type group with eigenvalue map  $\eta$ , such that  $\text{im } \eta = \mu_{h'} \leq \mu_{2h}$ . There is a decomposition*

$$M_k(\Gamma_\eta) = \bigoplus_{\substack{\eta': \Gamma \rightarrow \mu_{2h} \\ \ker \eta' \supseteq \Gamma_\eta}} M_k(\Gamma, \eta') = \bigoplus_{a=0}^{h'-1} M_k(\Gamma, \eta^{\sigma_a}).$$

**Proof.** Since  $\Gamma/\Gamma_\eta \cong \text{im } \eta$  is finite and abelian, the action of  $\Gamma$  on  $M_k(\Gamma_\eta)$  can be simultaneously diagonalized.  $\blacksquare$

Let  $\Gamma$  be a  $p^\alpha n|h$ -type group with eigenvalue map  $\eta$  such that  $\Gamma_\eta$  is genus zero and  $p \nmid nh$ . Lemma 2.2 tells us under which group  $\mathcal{T}|U_p$  is modular. We know that  $\mathcal{T}|U_p$  is weakly holomorphic, and next characterize the cusps at which it may be unbounded. We first recall that a set of representatives for the cusps of  $\Gamma_0(N)$  is given by

$$\left\{ \frac{a}{b} : b|N, a \in \mathbb{Z} \right\} / \sim, \quad \text{where } \frac{a}{b} \sim \frac{c}{d} \iff b = d \quad \text{and} \quad a \equiv c \pmod{\gcd(b, N/b)}.$$

Moreover, if two cusps  $\frac{a}{b}$  and  $\frac{c}{d}$  (not necessarily representatives of the form above) are equivalent under  $\Gamma_0(N)$  and  $\gcd(a, b) = \gcd(c, d) = 1$ , then  $\gcd(b, N) = \gcd(d, N)$ . Both of these facts follow from [13, Proposition 3.8.3].

In what follows, if  $\Gamma \leq \text{GL}_2^+(\mathbb{R})$  is commensurable with  $\text{SL}_2(\mathbb{Z})$  and  $s, s' \in \mathbb{P}^1(\mathbb{Q})$  are cusps, then we write

$$s \stackrel{\Gamma}{\sim} s'$$

to mean that  $s$  and  $s'$  are equivalent under  $\Gamma$ . If  $\Gamma = \Gamma_0(N)$  then we simply write  $s \stackrel{N}{\sim} s'$ .

**Lemma 2.4.** *Let  $p \nmid nh$  be prime, and let  $\Gamma$  be a  $p^\alpha n|h$ -type group with eigenvalue map  $\eta$ . Let  $\Gamma'$  and  $\eta'$  be the  $p^\beta n|h$ -type group and eigenvalue map defined in Lemma 2.2(b). Suppose  $f$  is a weakly holomorphic modular form on  $\Gamma$  with eigenvalue map  $\eta$ , so that  $f|U_p$  is on  $\Gamma'$  with eigenvalue map  $\eta'$  by Lemma 2.2.*

(a) *If  $f$  is bounded away from  $\infty$  then the poles of  $f|U_p$  are supported on the cusps*

$$\{\infty\} \cup \{s : s \stackrel{p}{\sim} 0\} \quad \text{of } \Gamma'_{\eta'}.$$

(b) *Suppose that  $p \nmid e$  for all  $e \in \text{AL}(\Gamma)$ . If the poles of  $f$  are supported on  $\{\infty\} \cup \{s : s \stackrel{p}{\sim} 0\}$  then the same is true of  $f|U_p$ .*

(c) *Suppose that  $\alpha \geq 2$  and  $p \nmid e$  for all  $e \in \text{AL}(\Gamma)$ . If  $f$  is bounded away from  $\infty$  and  $f|U_p$  is bounded at  $\infty$ , then  $f|U_p$  is constant.*

**Proof.** We begin with part (a). Suppose that  $f$  is bounded away from  $\infty$ , and suppose that  $f|U_p$  is unbounded at the cusp  $s$ . If  $s \stackrel{p}{\sim} 0$  then we are done. Thus we may assume that  $s \stackrel{p}{\sim} \infty$ . Also, by (2.3), we must have  $S_\mu \cdot s \stackrel{\Gamma_\eta}{\sim} \infty$  for some  $\mu$ . Equivalently,  $s \stackrel{p^\alpha nh}{\sim} S_\mu^{-1} A \cdot \infty$  for some  $A$  that can be expressed as a word in the matrices

$$x = \begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ p^\alpha n & 1 \end{pmatrix}, \quad \text{and} \quad W_e \in \Gamma_\eta$$



of Section 2.1. Since  $W_e$  normalizes  $\Gamma_0(p^\alpha n|h)$  (see [17, Theorem 2.7]), we may write all of the  $W_e$ 's on the right of  $A$ . By cancelling  $W_{p^\alpha}$ 's, we can moreover demand that  $p \nmid e$  for all  $W_e$  appearing in  $A$ , for otherwise we would have  $A \cdot \infty \stackrel{p}{\sim} 0$  while  $S_\mu \cdot s \stackrel{p}{\sim} \infty$ . As in the proof of Lemma 2.2, we can write  $S_\mu^{-1}A = A'S_\mu^{-1}V$  for some  $V \in \Gamma_0(p^\alpha nh)$ , where  $A'$  is obtained from  $A$  by replacing each  $x$  with  $x^p$  and each  $y$  with  $y^p$ . Hence  $s \stackrel{p^\alpha nh}{\sim} A'S_\nu^{-1} \cdot \infty$ .

If  $\alpha \leq 1$  and  $\beta = 1$  then either  $S_\nu^{-1} \cdot \infty \stackrel{p^\beta nh}{\sim} \infty$  or  $\frac{1}{nh}$ . But since  $A' \cdot \frac{1}{nh} \stackrel{p}{\sim} 0$ , we must have  $S_\nu^{-1} \cdot \infty \stackrel{p^\beta nh}{\sim} \infty$ . Hence  $s \stackrel{p^\beta nh}{\sim} A' \cdot \infty \stackrel{\Gamma'_{\eta'}}{\sim} \infty$ , as desired. The case  $\alpha \geq 2$  is dealt with similarly, completing the proof of (a).

A similar argument gives part (b), where we must now use the fact that  $p \nmid e$  for  $e \in \text{AL}(\Gamma)$  to show that  $p \nmid e$  for all  $W_e$  appearing in  $A$ . For part (c), one finds that  $f|U_p$  may only have a pole at the cusp  $\infty$ ; however, since it does not have a pole here by hypothesis,  $f|U_p$  is bounded everywhere and hence constant. ■

**Remark 2.5.** Lemma 2.4(c) delivers a class of Hauptmoduln  $\mathcal{T}$  for which  $\mathcal{T}|U_p = 0$ . For the Hauptmoduln from monstrous moonshine to which this applies, this property also follows from [30, Lemma 3.2]. Furthermore, if  $\Gamma$  is a  $n|h$ -type group and  $\eta$  is an eigenvalue map with  $\eta(x) = e^{2\pi im/h}$ , then any meromorphic modular form  $f = \sum_{n=m}^{\infty} a(n)q^n$  on  $\Gamma$  with eigenvalue map  $\eta$  has  $a(n) = 0$  if  $n \not\equiv m \pmod{h}$ , since  $x$  sends  $q \mapsto e^{2\pi im/h}q$ . In particular, if  $h \equiv 0 \pmod{p}$  and  $\mathcal{T}$  is the Hauptmoduln on  $\Gamma_\lambda$ , then  $f|U_p = 0$ .

Inspection of Table A.1 shows that the only monster Hauptmoduln with  $\mathcal{T}|U_p = 0$  are those with  $h \equiv 0 \pmod{p}$  and those coming from Lemma 2.4(c).

In Section 3 we will need a modular form  $g$  on an  $n|h$ -type group  $\Gamma$  such that the zeros of  $g$  can cancel the poles of  $\mathcal{T}|U_p$ , whose locations were just determined. We will also need  $g$  to have certain properties modulo  $p$ .

To construct  $g$ , we will use the *modular discriminant*  $\Delta(\tau) = q \prod_{n \geq 1} (1 - q^n)^{24}$ . If a modular form  $f = \sum_{n=m}^{\infty} a(n)q^n$  has rational coefficients, we set  $v_p(f) = \inf_n v_p(a_n)$  where  $v_p(a_n) = \sup\{r \in \mathbb{Z} : p^r \mid a_n\}$ .

**Lemma 2.6.** *Let  $\Gamma$  be a  $pn|h$ -type group where  $p \nmid nh$  is prime and  $p \nmid e$  for all  $e \in \text{AL}(\Gamma)$ . Let  $m = \#\text{AL}(\Gamma)$  and set  $a = 12m(p - 1)$ . Then there is a modular form  $g$  on  $\Gamma$  of weight  $a$  with rational coefficients such that*

- (a)  $g \equiv 1 \pmod{p}$ ,
- (b)  $v_p(g|_a W_p) \geq 6m(p + 1)$ ,
- (c) *As a function on  $\Gamma_0(pnh)$ ,  $g$  vanishes to order  $\geq m(p^2 - 1)$  at every cusp equivalent to 0 under  $\Gamma_0(p)$ .*

Specifically,  $g$  can be chosen to be

$$\prod_{e \in \text{AL}(\Gamma)} \left. \frac{\Delta(h\tau)^p}{\Delta(ph\tau)} \right|_{12(p-1)} W_e.$$

**Proof.** First, let

$$g_p(\tau) = \frac{\Delta(h\tau)^p}{\Delta(ph\tau)}$$

and  $a_p = 12(p-1)$ . Note that  $g_p(\tau)$  is invariant under  $\Gamma_0(pn|h)$ . For any  $e \in \text{AL}(\Gamma)$

$$(g_p|_{a_p} W_e)(\tau) = \frac{(\Delta(h\tau)|_{12} W_e)^p}{\Delta(p h \tau)|_{12} W_e} = \left(\frac{h * e}{h}\right)^{6(p-1)} \frac{\Delta((h * e)\tau)^p}{\Delta(p(h * e)\tau)} \quad (2.5)$$

by (2.2). On the other hand, we see that

$$(g_p|_{a_p} W_{pe})(\tau) = p^{6(p+1)} \left(\frac{h * e}{h}\right)^{6(p-1)} \frac{\Delta(p(h * e)\tau)^p}{\Delta((h * e)\tau)}. \quad (2.6)$$

Since  $\Delta$  is nonzero on  $\mathbb{H}$ , (2.5) shows that  $g_p|_{a_p} W_e$  is a modular form on  $\Gamma_0(pnh)$  with rational coefficients. Moreover, (2.6) shows that each  $g_p|_{a_p} W_{pe}$  for  $e \in \text{AL}(\Gamma)$  vanishes to order  $(h * e)(p^2 - 1)$  at  $\infty$ , so that each  $g_p|_{a_p} W_e$  vanishes to order  $\geq p^2 - 1$  at the cusps  $s \stackrel{\mathcal{L}}{\sim} 0$ .

Since  $(1 - q^n)^p \equiv 1 - q^{np} \pmod{p}$ , we see that  $g_p|_{a_p} W_e \equiv \left(\frac{h * e}{h}\right)^{6(p-1)} \equiv 1 \pmod{p}$ . Moreover  $v_p(g_p|_{a_p} W_p) = 6(p+1)$ . Thus, we may set

$$g = \prod_{e \in \text{AL}(\Gamma)} g_p|_{a_p} W_e,$$

which clearly satisfies the conditions given. ■

**Remark 2.7.** The function in Lemma 2.6 is chosen for its large order zeroes, in contrast with symmetrizations of the function  $g = E_a - p^{a/2} E_a|_a W_p$  of [37, Lemma 8]. This will be computationally useful in Section 4.

We conclude with a few tools for working with  $q$ -expansions of mod  $p$  modular forms.

**Lemma 2.8** (Sturm's bound [39]). *Let  $f \in M_k(\Gamma_0(N))$  with integer coefficients  $a_n$ . If  $p \nmid a_n$  for  $p \leq (k/12)[\text{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$ , then  $p \mid a_n$  for all  $n$ .*

We will apply Sturm's bound to weakly holomorphic modular forms after multiplying by a power of the function from Lemma 2.6. We thus bound the pole orders of  $\mathcal{T}|U_p$ .

**Lemma 2.9.** *Let  $f$  be a weakly holomorphic function on  $X_0(p^\alpha N)$ , where  $p \nmid N$ , and let  $\beta = \max\{\alpha, 1\}$ . If  $r$  is the maximum order of a pole of  $f$  on  $X_0(p^\alpha N)$ , then the poles of  $f|U_p$  as a function on  $X_0(p^\beta nh)$  have order at most  $rp^2$  when  $\alpha = 0$ , and order at most  $rp$  otherwise.*

**Proof.** The ramification index of each cusp of  $X_0(pnh)$  over  $X_0(nh)$  is a divisor of  $p$ . Thus, for the case  $\alpha = 0$ , the maximum order of a pole of  $f$  pulled back to  $X_0(pnh)$  is  $rp$ . The  $U_p$  operator may be defined via the correspondence

$$\begin{array}{ccc} (\Gamma_0(p^\beta nh) \cap \gamma^{-1} \Gamma_0(p^\beta nh) \gamma) \backslash \mathbb{H}^* & \xrightarrow{\sim} & (\gamma \Gamma_0(p^\beta nh) \gamma^{-1} \cap \Gamma_0(p^\beta nh)) \backslash \mathbb{H}^* \\ \downarrow & & \downarrow \\ X_0(p^\beta nh) & & X_0(p^\beta nh) \end{array}$$

where  $\gamma = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ . The projections have degree  $p$ , so  $\mathcal{T}$  pulls back to a function on  $(\gamma \Gamma_0(p^\beta nh) \gamma^{-1} \cap \Gamma_0(p^\beta nh)) \backslash \mathbb{H}^*$  with poles at most degree  $rp^2$  when  $\alpha = 0$  and  $rp$  else. The other maps of the correspondence, which are pullback by the isomorphism and trace down to  $X_0(p^\beta nh)$ , do not increase the maximum pole order, so the claim follows. ■

### 2.3 Trace formulas

Following Serre's idea [37], we will apply the trace to view classical modular forms as  $p$ -adic modular forms of lower level. In this section we discuss a few properties of trace maps.

Suppose  $\Gamma$  and  $\Gamma'$  are subgroups of  $\mathrm{GL}_2^+(\mathbb{R})$  with  $\Gamma$  a finite index subgroup of  $\Gamma'$ . We define the *trace*  $\mathrm{Tr}_{\Gamma \backslash \Gamma'}$  from  $\Gamma$  to  $\Gamma'$  to be the operation

$$\mathrm{Tr}_{\Gamma \backslash \Gamma'} f = \sum_{i=1}^m f|_k \gamma_i, \tag{2.7}$$

where  $\{\gamma_1, \dots, \gamma_m\}$  is a system of right coset representatives for  $\Gamma \backslash \Gamma'$ . If  $f$  is modular on  $\Gamma$  then  $\mathrm{Tr}_{\Gamma \backslash \Gamma'}$  is modular on the larger group  $\Gamma'$ . When  $\Gamma = \Gamma_0(N)$  and  $\Gamma' = \Gamma_0(N')$ , we simply write  $\mathrm{Tr}_{N \backslash N'}$  for  $\mathrm{Tr}_{\Gamma \backslash \Gamma'}$ .

First consider  $\Gamma = \Gamma_0(pN)$  and  $\Gamma' = \Gamma_0(N)$ . The following generalizes [37, Lemma 7].

**Lemma 2.10.** *Let  $p \nmid N$  be prime.*

(a) *A set of representatives for  $\Gamma_0(pN) \backslash \Gamma_0(N)$  is given by*

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 1 & \lambda \\ N & N\lambda + 1 \end{pmatrix} : 1 \leq \lambda \leq p \right\}.$$

(b) *If  $f$  is a weight  $k$  modular form on  $\Gamma_0(pN)$  then*

$$\mathrm{Tr}_{pN \backslash N} f = f + p^{1-k/2} (f|_k W_p)|_{U_p}$$

where  $W_p$  is the corresponding Atkin–Lehner involution on  $\Gamma_0(pN)$ .

**Proof.** Since  $[\Gamma_0(N) : \Gamma_0(pN)] = p + 1$ , part (a) follows upon checking that the representatives are inequivalent modulo  $\Gamma_0(pN)$ . One can also check that for any  $1 \leq \lambda \leq p$ , if  $\mu \equiv N^{-1} \pmod{p}$ , then

$$\begin{pmatrix} 1 & \lambda \\ N & N\lambda + 1 \end{pmatrix} = V W_p \begin{pmatrix} 1/p & (\lambda + \mu)/p \\ 0 & 1 \end{pmatrix}$$

for some  $V \in \Gamma_0(pN)$ . Part (b) follows from this. ■

The remainder of this section will extend Lemma 2.10 to the more general context we need, for example tracing from  $\Gamma_0(pN)+e, \dots$  to  $\Gamma_0(N)+e, \dots$  for  $p \nmid N$ . More precisely, for a prime  $p \nmid nh$ , suppose that  $\Gamma$  is a  $pn|h$ -type group with eigenvalue map  $\eta$  with  $p \nmid e$  for all  $e \in \mathrm{AL}(\Gamma)$ . Let  $\Gamma'$  be the  $n|h$ -type group such that  $\mathrm{AL}(\Gamma') = \mathrm{AL}(\Gamma)$ . We have  $\Gamma \subset \Gamma'$ , and can take  $\eta'$  to be the eigenvalue map on  $\Gamma'$  with  $\eta'|_{\Gamma} = \eta$ . Since  $\Gamma'$  is generated by

$$x = \begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}, \quad W_e \text{ such that } e \in \mathrm{AL}(\Gamma') = \mathrm{AL}(\Gamma)$$

as in Section 2.1, this uniquely determines  $\eta'$ . Then [17, Lemma 2.3] and [17, Theorem 2.7] together imply that the inclusion of representatives

$$\iota: \Gamma/\Gamma_0(pnh) \hookrightarrow \Gamma'/\Gamma_0(nh)$$

is an isomorphism. We set  $H = \mathrm{im}(\iota|_{\Gamma_\eta}) \leq \Gamma'$ , and consider the restricted isomorphism

$$\iota|_{\Gamma_\eta}: \Gamma_\eta/\Gamma_0(pnh) \xrightarrow{\sim} H/\Gamma_0(nh). \tag{2.8}$$

We have that  $H \leq \Gamma'_{\eta'}$ . Moreover,  $\mathrm{im} \eta' = \mathrm{im} \eta$ , so  $[\Gamma' : \Gamma'_{\eta'}] = [\Gamma : \Gamma_\eta] = [\Gamma' : H]$  and thus  $\Gamma'_{\eta'} = H$ . We have nearly proved the following lemma.

**Lemma 2.11.** *Let  $\Gamma$  be a  $pn|h$ -type group with eigenvalue map  $\eta$  such that  $p \nmid e$  for all  $e \in \text{AL}(\Gamma)$ . Let  $\Gamma'$  be an  $n|h$ -type group with  $\text{AL}(\Gamma') = \text{AL}(\Gamma)$  with eigenvalue map  $\eta'$  such that  $\eta'|_{\Gamma} = \eta$ . Then for any weight  $k$  modular form on  $\Gamma_\eta$  we have*

$$\text{Tr}_{\Gamma_\eta \backslash \Gamma'_\eta} f = \text{Tr}_{pnh \backslash nh} f = f + p^{1-k/2}(f|_k W_p)|_{U_p}.$$

**Proof.** We need to show  $\text{Tr}_{\Gamma_\eta \backslash \Gamma'_\eta} f = \text{Tr}_{pnh \backslash nh} f$ . Let  $\{\gamma_i\}$  be any set of representatives for  $\Gamma_0(pnh) \backslash \Gamma_0(nh)$ . Then  $\{\gamma_i\}$  is also a set of representatives for  $\Gamma_\eta \backslash \Gamma'_\eta$ . Indeed, by the isomorphism (2.8) we have  $[\Gamma'_\eta : \Gamma_\eta] = [\Gamma_0(nh) : \Gamma_0(pnh)]$  so it suffices to check that no two  $\gamma_i$  are equivalent. Suppose  $\gamma_i \gamma_j^{-1} \in \Gamma_\eta$ . Then  $\gamma_i \gamma_j^{-1} \in \Gamma \cap \Gamma_0(nh) = \Gamma_0(pnh)$  so that  $\gamma_i = \gamma_j$  as desired. The formula then follows from Lemma 2.10.  $\blacksquare$

**Remark 2.12.** Lemma 2.11 only assumes that  $f$  is on  $\Gamma_\eta$ . Under the stronger assumption that  $f$  is on  $(\Gamma, \eta)$ , we obtain the finer result that  $\text{Tr}_{pnh \backslash nh} f$  is on  $(\Gamma', \eta')$ . To see this, let  $x$  and  $Y = y^p$  be the generators of  $\Gamma_0(pn|h)/\Gamma_0(pnh)$ , and choose appropriate representatives of  $W_e$  which normalize  $\Gamma_0(nh)$ . Then, apply  $x, Y$ , and  $W_e$  to both sides of (2.7).

### 3 $p$ -adic modular forms

In this section, we extend of Serre's theory of  $p$ -adic modular forms from [37] to Hauptmoduln and  $n|h$ -type groups. In particular, we study the interaction between eigenvalue maps and the mod  $p$  weight filtration. These  $p$ -adic properties could be studied by extending the theory of Katz and others, but we choose to generalize Serre's original treatment in order to perform explicit calculations for our applications. Take  $p \geq 5$ , and let  $\Gamma$  be an  $n|h$ -type group with eigenvalue map  $\eta$ . We first study  $M_k(\Gamma, \eta)$  and its  $p$ -adic completion. In Section 3.1 we prove that Hauptmoduln  $\mathcal{T}$  become  $p$ -adic modular forms on some  $(\Gamma', \eta')$  under applications of  $U_p$ . In Section 3.2 we extract structural results concerning ordinary spaces and the action of  $U_p$  on these  $p$ -adic modular forms. Again, readers interested only in modular groups of the form  $\Gamma_0(N)+e, \dots$  can take  $h = 1$  and let eigenvalue maps be identically 1.

For an  $n|h$ -type group  $\Gamma$  with eigenvalue map  $\eta: \Gamma \rightarrow \mu_{2h}$ , we first define the spaces:

- (1)  $M_k^{\mathbb{Q}}(\Gamma, \eta) = M_k(\Gamma, \eta) \cap \mathbb{Q}[[q]]$ , the  $\mathbb{Q}$ -vector space of modular forms with rational  $q$ -expansion;
- (2)  $M_k^{(p)}(\Gamma, \eta) = M_k(\Gamma, \eta) \cap \mathbb{Z}_{(p)}[[q]]$ , the  $\mathbb{Z}_{(p)}$ -module of modular forms with  $p$ -integral  $q$ -expansion; and
- (3)  $\tilde{M}_k(\Gamma, \eta) = M_k^{(p)}(\Gamma, \eta) \otimes \mathbb{F}_p$ , the  $\mathbb{F}_p$ -vector space obtained by reducing  $M_k^{(p)}(\Gamma, \eta) \bmod p$ .

Similarly define  $M_k^{\mathbb{Q}}(\Gamma_\eta)$ ,  $M_k^{(p)}(\Gamma_\eta)$ , and  $\tilde{M}_k(\Gamma_\eta)$ . If  $f$  reduces mod  $p$  to a form in  $\tilde{M}_k(\Gamma, \eta)$ , we abuse notation and write  $f \in \tilde{M}_k(\Gamma, \eta)$ , and similarly for  $\Gamma_\eta$ . We focus on  $M_k(\Gamma, \eta)$ , and the corresponding results for  $M_k(\Gamma_\eta)$  follow from Lemma 2.3.

Following [37], we define a  $p$ -adic modular form on  $(\Gamma, \eta)$  to be a  $q$ -expansion  $f \in \mathbb{Q}_p[[q]]$  admitting a sequence  $f_m \in M_{k_m}^{\mathbb{Q}}(\Gamma, \eta)$  that converges  $p$ -adically with  $v_p(f_m - f) \rightarrow \infty$ , i.e.,

$$\lim_{m \rightarrow \infty} f_m = f.$$

Similarly, a  $p$ -adic modular form on  $\Gamma$  is a  $p$ -adic modular form on  $(\Gamma, \mathbf{1})$ .

For any  $N$ , if  $f, f'$  are modular forms on  $\Gamma_0(N)$  of weight  $k, k'$  and  $f \equiv f' \pmod{p^n}$  then  $k \equiv k' \pmod{p^{n-1}(p-1)}$  (see [28, Corollary 4.4.2]). It follows that the weight of a  $p$ -adic modular form on  $\Gamma_0(N)$ , defined as the limit of the  $k_m$  in the space

$$\mathfrak{X} = \varprojlim \mathbb{Z}/p^n \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z},$$

exists and does not depend on the choice of sequence  $(f_m)$ . The same is true of  $p$ -adic modular forms on  $(\Gamma, \eta)$ , since  $M_k(\Gamma, \eta) \subseteq M_k(\Gamma_0(nh))$ . In particular, forms in  $M_k(\Gamma, \eta)$  have trivial nebentypus, as required in [28].

The correct extension of the mod  $p$  weight filtration to modular forms for  $n|h$ -type groups will feature a quadratic twist. To this end, we first twist our eigenvalue maps.

**Definition 3.1.** Let  $\Gamma$  be an  $n|h$  type group and  $p \nmid nh$  a prime. If  $\eta$  is an eigenvalue map on  $\Gamma$ , then the *twist* of  $\eta$  is the map  $\eta_t: \Gamma \rightarrow \mu_{2h}$  defined by

$$\eta_t(\gamma) = \eta(\gamma) \quad \text{for } \gamma \in \Gamma_0(n|h) \quad \text{and} \quad \eta_t(W_e) = \left(\frac{e}{p}\right) \eta(W_e) \quad \text{for } e \in \text{AL}(\Gamma),$$

where  $\left(\frac{\cdot}{p}\right)$  denotes the Legendre symbol.

**Remark 3.2.** If  $\mathbf{1}$  denotes the trivial eigenvalue map  $\mathbf{1}(\gamma) = 1$  for all  $\gamma$ , then  $\eta_t = \eta \mathbf{1}_t$  for all  $\eta$ . Also, if  $\left(\frac{e}{p}\right) = 1$  for all  $e \in \text{AL}(\Gamma)$  then  $\eta = \eta_t$ .

Below, we collect some useful facts and begin to see the relationship between eigenvalue map twists and the weight mod  $2(p-1)$ . Let  $E_k(\tau)$  denote the weight  $k$  *Eisenstein series* with constant term 1.

**Proposition 3.3.** *Let  $\Gamma$  be an  $n|h$ -type group with eigenvalue map  $\eta$ , and let  $p \geq 5$  be prime with  $p \nmid nh$ .*

(a) *Let  $F(\tau) = E_{p-1}(h\tau)$ . Then*

$$\hat{F} = \sum_{e \in \text{AL}(\Gamma)} \left(\frac{e}{p}\right) F|_{p-1} W_e \in M_{p-1}(\Gamma, \mathbf{1}_t)$$

*is congruent to  $\#\text{AL}(\Gamma) \pmod{p}$ .*

(b) *For all  $k$ , we have the inclusions*

$$\tilde{M}_k(\Gamma, \eta) \subseteq \tilde{M}_{k+p-1}(\Gamma, \eta_t) \subseteq \tilde{M}_{k+2(p-1)}(\Gamma, \eta) \subseteq \tilde{M}_{k+3(p-1)}(\Gamma, \eta_t) \subseteq \dots$$

(c) *Suppose  $\eta \neq \eta_t$ . Then for  $f \in M_k^{\mathbb{Q}}(\Gamma, \eta)$  and  $f' \in M_{k'}^{\mathbb{Q}}(\Gamma, \eta)$  we have that*

$$0 \neq f \equiv f' \pmod{p^n} \quad \text{implies} \quad k \equiv k' \pmod{2p^{n-1}(p-1)}.$$

(d) *If  $\eta \neq \eta_t$  then the weight of a  $p$ -adic modular form on  $(\Gamma, \eta)$  is well-defined as an element of  $\hat{\mathfrak{X}} = \mathbb{Z}_p \times \mathbb{Z}/(2p-2)\mathbb{Z}$ .*

**Proof.** Since  $F$  is invariant under  $\Gamma_0(n|h)$ , the statement that  $\hat{F} \in M_{p-1}(\Gamma, \mathbf{1}_t)$  becomes

$$\hat{F}|W_e = \left(\frac{e}{p}\right) F,$$

which follows from multiplicativity of the Legendre symbol. We also have

$$F|_{p-1} W_e(\tau) = \left(\frac{h * eh^2}{h}\right)^{\frac{p-1}{2}} E_{p-1}((h * eh^2)\tau) \equiv \left(\frac{e}{p}\right) \pmod{p}$$

since  $E_{p-1} \equiv 1 \pmod{p}$  (see [37, Section 1]). Thus  $\hat{F} \equiv \sum_{e \in \text{AL}(\Gamma)} 1 \pmod{p}$ , giving part (a).

Since  $p \neq 2$ , this implies  $1 \in \tilde{M}_{p-1}(\Gamma, \mathbf{1}_t)$ , giving part (b) since  $\eta \mathbf{1}_t = \eta_t$  and

$$M_k(\Gamma, \eta) \cdot M_{k'}(\Gamma, \eta') = M_{k+k'}(\Gamma, \eta\eta').$$

For part (c), we already know  $k \equiv k' \pmod{p^{n-1}(p-1)}$ . Assume without loss of generality that  $k \leq k'$ . If  $k \not\equiv k' \pmod{2p-2}$  then by part (b) there exists  $g \in M_{k'}^{\mathbb{Q}}(\Gamma, \eta_t)$  with  $g \equiv f \pmod{p}$ . Since  $\eta \neq \eta_t$ , let  $e \in \text{AL}(\Gamma)$  be a quadratic nonresidue so that

$$\eta(W_e)f' = f'|_{|k'}W_e \equiv g|_{|k'}W_e = -\eta(W_e)g \equiv -\eta(W_e)f' \pmod{p},$$

which implies  $f' \equiv f \equiv 0 \pmod{p}$ . Part (d) then follows.  $\blacksquare$

This motivates the following  $\mathbb{F}_p$ -spaces, which incorporate these twisted inclusions. Set

$$\tilde{M}(\Gamma, \eta)^\alpha = \bigcup_{k \equiv \alpha \pmod{2p-2}} \tilde{M}_k(\Gamma, \eta) \cup \bigcup_{k \equiv \alpha + p - 1 \pmod{2p-2}} \tilde{M}_k(\Gamma, \eta_t)$$

for  $\alpha \in \mathbb{Z}/(2p-2)\mathbb{Z}$ . If every  $e \in \text{AL}(\Gamma)$  is a quadratic residue mod  $p$ , we have  $\eta = \eta_t$ , and  $\tilde{M}(\Gamma, \eta)^\alpha$  only depends on  $\alpha \pmod{p-1}$ .

### 3.1 Producing $p$ -adic modular forms from Hauptmoduln

Let  $\Gamma$  be a  $p^\alpha n|h$ -type group with eigenvalue map  $\eta$  where  $p \nmid nh$  is prime. Suppose  $\Gamma_\eta$  is genus zero, and its Hauptmodul  $\mathcal{T}$  is on  $\Gamma$  with eigenvalue map  $\eta$ . We show that for some  $\beta$ ,  $\mathcal{T}|U_p^\beta$  is a  $p$ -adic modular form on  $(\Gamma', \eta')$  for some specified  $n|h$ -type group  $\Gamma'$  and eigenvalue map  $\eta'$ . We can take  $\beta = 1$  whenever  $\alpha \leq 3$ .

**Lemma 3.4.** *Let  $\Gamma$  be a  $p^\alpha n|h$ -type group for  $p \nmid nh$  prime, and  $\eta$  be an eigenvalue map on  $\Gamma$ . Let  $f$  be a weight 0 weakly holomorphic modular form on  $(\Gamma, \eta)$  that is holomorphic away from  $\infty$ . Let  $\Gamma'$  be the  $n|h$ -type group with  $e \in \text{AL}(\Gamma')$  if and only if  $e \in \text{AL}(\Gamma)$  and  $p \nmid e$ . Let  $\beta = \max\{1, \alpha - 1\}$ , and let  $\eta'$  be the eigenvalue map on  $\Gamma'$  such that*

$$\eta'(x) = \eta(x^{p^\beta}), \quad \eta'(y') = \eta(y^{p^{\alpha+\beta}}), \quad \eta'(W_e) = \eta(W_e) \quad \text{for } e \in \text{AL}(\Gamma'),$$

where  $x, y, y'$  are the generators of  $\Gamma_0(p^\alpha n|h)$  and  $\Gamma_0(n|h)$  given by

$$x = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ p^\alpha n & 1 \end{pmatrix}, \quad y' = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}.$$

Then,  $f|U_p^\beta$  is  $p$ -adic modular form of weight 0 on  $(\Gamma', \eta')$ .

**Proof.** By Lemma 2.2,  $f|U_p^\beta$  is a weakly holomorphic modular form on  $(\Gamma, \nu)$  where  $\Gamma$  is the  $pn|h$ -type group  $\Gamma$  where  $e \in \text{AL}(G)$  if and only if  $e \in \text{AL}(\Gamma)$  and  $p \nmid e$ , and  $\nu$  satisfies

$$\nu(x) = \eta(x^{p^\beta}), \quad \nu(Y) = \eta(y^{p^{\alpha+\beta-1}}), \quad \nu(W_e) = \eta(W_e), \quad \text{where } Y = \begin{pmatrix} 1 & 0 \\ pn & 1 \end{pmatrix}.$$

The remainder of the proof follows [37, Theorem 10]. To show that  $f|U_p^\beta$  is a  $p$ -adic modular form on  $(\Gamma', \eta')$ , we set for  $m \geq 0$

$$f_m = \text{Tr}_{G_\nu \setminus \Gamma'_\eta} (f|U_p^\beta g^{p^m}) = \text{Tr}_{pnh \setminus nh} (f|U_p^\beta g^{p^m}),$$

where  $g$  is the modular form on  $\Gamma$  given by Lemma 2.6. Since

$$\begin{aligned} \eta'(x) = \nu(x) = \eta(x^{p^\beta}) \quad \text{and} \quad \eta'(y') = \nu(Y^p) = \eta(y^{p^{\alpha+\beta}}) \quad \text{and} \\ \eta'(W_e) = \nu(W_e) = \eta(W_e) \quad \text{for} \quad e \in \text{AL}(\Gamma') \end{aligned}$$

we know  $f_m$  is a weakly holomorphic modular form on  $(\Gamma', \eta')$  by Lemma 2.11. Lemma 2.4 shows that  $f|U_p^\beta$  has poles only at the cusps equivalent to 0 on  $\Gamma_0(p)$ , and since  $g$  has zeros at all such cusps, we know  $f|U_p^\beta g^m$  is holomorphic for  $m$  sufficiently large. If  $a$  is the weight of  $g$ , the weight of  $f_m$  is  $ap^m$ , which  $p$ -adically converges to 0. Hence it suffices to show that  $f_m \rightarrow f|U_p^\beta$  in the  $p$ -adic limit. We compute that

$$\begin{aligned} f_m - f|U_p^\beta &= (f_m - f|U_p^\beta g^{p^m}) + f|U_p^\beta (g^{p^m} - 1), \\ v_p(f_m - f|U_p^\beta) &\geq \min \{v_p(f_m - f|U_p^\beta g^{p^m}), v_p(f|U_p^\beta) + v_p(g^{p^m} - 1)\}. \end{aligned}$$

Since  $g^{p^m} \equiv 1 \pmod{p^{m+1}}$ , we have  $v_p(f|U_p^\beta) + v_p(g^{p^m} - 1) \geq m + 1$ . Lemma 2.11 implies

$$f_m - f|U_p^\beta g^{p^m} = p^{1-ap^m/2} (f|U_p^\beta g^{p^m} |_{ap^m} W_p) |U_p,$$

and since applying  $U_p$  does not decrease the power of  $p$  dividing a  $q$ -expansion, we have

$$\begin{aligned} v_p(f_m - f|U_p^\beta g^{p^m}) &\geq 1 - \frac{ap^m}{2} + v_p(f|U_p^\beta |_0 W_p) + p^m v_p(g|_a W_p) \\ &\geq 1 + v_p(f|U_p^\beta |_0 W_p) + p^m \left( v_p(g|_a W_p) - \frac{a}{2} \right). \end{aligned}$$

Lemma 2.6 gives  $v_p(g|_a W_p) > \frac{a}{2}$ . Hence,  $v_p(f_m - f|U_p^\beta) \rightarrow \infty$  as  $m \rightarrow \infty$ , as desired. ■

**Remark 3.5.** If  $\Gamma$  is a  $p^\alpha n|h$ -type group with eigenvalue map  $\eta$  such that  $\Gamma_\eta$  is genus zero, and the Hauptmodul  $\mathcal{T}$  on  $\Gamma_\eta$  is on  $(\Gamma, \eta)$ , then Lemma 3.4 applies. Moreover, since  $\mathcal{T}^r$  is on  $(\Gamma, \eta^{\sigma^r})$ , the lemma also applies to powers of the Hauptmodul. In particular, polynomials in  $\mathcal{T}$  are  $p$ -adic modular forms on  $\Gamma'_{\eta'}$  after enough applications of  $U_p$ .

### 3.2 Ordinary spaces

Having produced  $p$ -adic modular forms from Hauptmoduln on certain  $n|h$ -type groups, we now study the action of  $U_p$ . The key idea, developed by Serre on level 1 in [37], is that  $U_p$  contracts mod  $p$  modular forms onto a finite-dimensional space. These structural results will allow us to verify  $p$ -adic annihilation of certain Hauptmoduln in Section 4.2.

We will take  $p \geq 5$  prime with  $p \nmid nh$ . For the Hecke operator  $T_p$ , we have

$$f|_k T_p = f|U_p + p^{k/2-1} f|_k A = f|U_p + p^{k-1} f(p\tau), \quad \text{where} \quad A = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix},$$

so  $f|U_p \equiv f|_k T_p \pmod{p}$  for  $k \geq 2$ . Since  $T_p$  acts on  $M_k(\Gamma_0(nh))$ , we know  $U_p$  acts on  $\tilde{M}_k(\Gamma_0(nh))$ . Furthermore, let  $\Gamma$  be an  $n|h$ -type group and  $\eta$  be an eigenvalue map. Since

$$Ax = x^p A, \quad Ay^p = yA, \quad AW_e = W_e A \quad \text{for} \quad p \nmid e,$$

Lemma 2.2 implies that  $T_p: M_k(\Gamma, \eta) \rightarrow M_k(\Gamma, \eta^{\sigma^p})$ . Hence  $U_p: \tilde{M}_k(\Gamma, \eta) \rightarrow \tilde{M}_k(\Gamma, \eta^{\sigma^p})$ , so we consider the space

$$\tilde{M}_k(\Gamma, [\eta]_p) = \tilde{M}_k(\Gamma, \eta) + \tilde{M}_k(\Gamma, \eta^{\sigma^p}),$$



which is stabilized by  $U_p$ . This sum is direct if and only if  $\eta \neq \eta^{\sigma_p}$ . We thus set

$$\tilde{M}(\Gamma, [\eta]_p)^\alpha = \tilde{M}(\Gamma, \eta)^\alpha + \tilde{M}(\Gamma, \eta^{\sigma_p})^\alpha$$

and remind the reader that  $\tilde{M}(\Gamma, \eta)^\alpha$  already encodes spaces with twisted eigenvalue map. We next show how  $U_p$  contracts  $\tilde{M}(\Gamma, [\eta]_p)^\alpha$  onto a finite-dimensional space called the *ordinary space*. Ordinary spaces of  $p$ -adic modular forms were extensively studied by Hida [25]. We describe our ordinary spaces in the language of Serre's  $p$ -adic modular forms.

**Proposition 3.6** (ordinary decomposition). *Let  $\Gamma$  be an  $n|h$ -type group with eigenvalue map  $\eta$ .*

(a) *We can write*

$$\tilde{M}(\Gamma, [\eta]_p)^\alpha = \mathfrak{S}(\Gamma, [\eta]_p)^\alpha \oplus \mathfrak{N}(\Gamma, [\eta]_p)^\alpha$$

*so that  $U_p$  is bijective on the ordinary space  $\mathfrak{S}(\Gamma, [\eta]_p)^\alpha$  and locally nilpotent on  $\mathfrak{N}(\Gamma, [\eta]_p)^\alpha$ ; that is, for any  $\mathfrak{N}(\Gamma, [\eta]_p)^\alpha$ , we have  $f|U_p^n = 0$  for  $n$  sufficiently large.*

(b) *Let  $4 \leq k \leq p+1$  be such that  $k \equiv \alpha \pmod{p-1}$ . If  $k \equiv \alpha \pmod{2p-2}$  then*

$$\mathfrak{S}(\Gamma, [\eta]_p)^\alpha \subseteq \tilde{M}_k(\Gamma, [\eta]_p).$$

*Otherwise,*

$$\mathfrak{S}(\Gamma, [\eta]_p)^\alpha \subseteq \tilde{M}_k(\Gamma, [\eta]_t)_p.$$

Proposition 3.6 can be interpreted to mean that repeated application of  $U_p$  reduces the weight of a modular form mod  $p$  to either 0 or  $p-1$ . To accomplish this, we need to incorporate the twisted eigenvalue maps. More precisely, the *filtration* of  $f \in \tilde{M}(\Gamma, [\eta]_p)^\alpha$  with respect to  $(\Gamma, \eta)$  is

$$w_{\Gamma, \eta}(f) = \min \{k : f \in \tilde{M}_k(\Gamma, [\eta]_p) \text{ or } \tilde{M}_k(\Gamma, [\eta]_t)_p\}.$$

When  $(\Gamma, \eta)$  is clear from context, we will simply write  $w$  for  $w_{\Gamma, \eta}$ . Similarly, the filtration  $w_\Gamma$  of a modular form mod  $p$  with respect to  $\Gamma$  is the filtration with respect to  $(\Gamma, \mathbf{1})$ .

To prove Proposition 3.6 we generalize the following fact from [27].

**Lemma 3.7.** *Suppose  $\Gamma = \Gamma_0(N)$ . Then for modular forms  $f$  mod  $p$  on  $\Gamma$  we have*

$$w_\Gamma(f|U_p) \leq p + \frac{w_\Gamma(f) - 1}{p}.$$

*In particular,  $w_\Gamma(f|U_p) < w_\Gamma(f)$  if  $w_\Gamma(f) > p+1$ .*

We give a suitable modification of Lemma 3.7 for  $(\Gamma, \eta)$ .

**Lemma 3.8.** *Let  $\Gamma$  be an  $n|h$ -type group with eigenvalue map  $\eta$ . For  $f \in \tilde{M}(\Gamma, [\eta]_p)^\alpha$ ,*

$$w_{\Gamma, \eta}(f|U_p) \leq p + \frac{w_{\Gamma, \eta}(f) - 1}{p}.$$

**Proof.** We first consider the special case  $\Gamma = \Gamma_0(n|h)$ . We proceed by induction on the finite index  $[\Gamma : \Gamma_0(nh)]$ . Suppose that for some  $\Gamma_0(nh) \leq \Gamma' \leq \Gamma_0(n|h)$  we have

$$w_{\Gamma', \eta|_{\Gamma'}}(f|U_p) \leq p + \frac{w_{\Gamma', \eta|_{\Gamma'}}(f) - 1}{p}. \quad (3.1)$$

Let  $T \in \Gamma_0(n|h)/\Gamma'$  be a representative for a nontrivial coset. Setting  $\Gamma'' = \langle \Gamma', T \rangle$  and  $\eta'' = \eta|\Gamma''$ , we will prove that (3.1) also holds for  $(\Gamma'', \eta'')$ .

Let  $f \in M_k^{(p)}(\Gamma'', [\eta'']_p) \subseteq M_k^{(p)}(\Gamma', [\eta|\Gamma']_p)$  be a modular form of filtration  $k$ . By assumption there is some  $g \in M_{k'}^{(p)}(\Gamma', [\eta|\Gamma']_p)$  with  $g \equiv f|U_p \pmod{p}$  and of filtration

$$k' \leq p + \frac{k-1}{p}.$$

Let  $t$  be the order of  $T$  in  $\Gamma''/\Gamma_0(nh)$ , and let  $\pi_m$  be the projection

$$\pi_m(g) = \frac{1}{t} \sum_{\ell=0}^{t-1} e^{-2\pi i \ell/t} g|_{k'} T^\ell$$

onto the  $e^{2\pi i m/t}$  eigenspace of  $T$ . Since  $p \geq 5$ , we know  $p \nmid t$ . Thus, if  $\varphi, \varphi'$  have the same weight and  $\varphi \equiv \varphi' \pmod{p}$ , then  $\pi_m(\varphi) \equiv \pi_m(\varphi') \pmod{p}$ .

By Proposition 3.3, multiplying by some power of  $\hat{F}$  gives  $f' \in M_{k'}^{(p)}(\Gamma', [\eta|\Gamma']_p)$  with  $f' \equiv g \pmod{p}$ . Since  $\hat{F}$  is invariant under  $\Gamma_0(n|h)$ , we have

$$\pi_m(g) \equiv \pi_m(f') \equiv \pi_m(f) \pmod{p}.$$

Let  $m$  be such that  $\eta(T) = e^{2\pi i m/t}$  and set

$$\pi = \begin{cases} \pi_m & \text{if } \pi_{pm} = \pi_m, \\ \pi_m \oplus \pi_{pm} & \text{otherwise,} \end{cases}$$

which is projection onto the span of the eigenspaces of  $T$  specified by  $[\eta]_p$ . Thus, we have  $\pi(g) \equiv \pi(f) = f \pmod{p}$ . Then  $\pi(g) \in M_{k'}^{(p)}(\Gamma'', [\eta'']_p)$  with  $\pi(g) \equiv f \pmod{p}$  as desired.

Extending by Atkin–Lehner involutions  $W_e$  is a similar computation. Define the projections as before, replacing  $T$  with the order  $t = 2$  action  $W_e$ . The function  $\hat{F}$  is not necessarily fixed by  $W_e$ , but rather lies in the  $\left(\frac{\varepsilon}{p}\right)$ -eigenspace of  $W_e$ . Thus

$$\pi_{m+\varepsilon}(g) = \pi_m(f') \equiv \pi_m(f) \pmod{p}$$

where  $\varepsilon = \frac{1}{2}(1 - \left(\frac{\varepsilon}{p}\right))$ , and we have  $\pi(g) \in M_{k'}^{(p)}(\Gamma'', [\eta'']_p)$  or  $\pi(g) \in M_{k'}^{(p)}(\Gamma'', [\eta'_t]_p)$ . ■

**Proof of Proposition 3.6.** Let  $k$  be as in the statement of Proposition 3.6. Set

$$\mathfrak{S}(\Gamma, [\eta]_p)^\alpha = \begin{cases} \bigcap_{n \geq 1} \text{im } U_p^n | \tilde{M}_k(\Gamma, [\eta]_p) & \text{if } k \equiv \alpha \pmod{2p-2}, \\ \bigcap_{n \geq 1} \text{im } U_p^n | \tilde{M}_k(\Gamma, [\eta_t]_p) & \text{otherwise.} \end{cases}$$

Also set

$$\mathfrak{N}(\Gamma, [\eta]_p)^\alpha = \bigcup_{n \geq 1} \ker U_p^n | \tilde{M}(\Gamma, [\eta]_p)^\alpha.$$

Lemma 3.8 shows that these spaces satisfy the conditions of the proposition. ■

Proposition 3.6 will be fundamental for proving  $p$ -adic annihilation in Section 4.

	2	3	5	7	11
1	20 2+5	1	1	1	1
2+	20 2+10	2+	2+	2+	3 3
2	22+	3+	3+	3 3	4 2+
3+	22+11	3	3 3	4 2+	11+
3 3	24 2+	3 3	4 2+	7+	
4+	24+	6+	5+	7	
4 2+	24 2+3	6+2	5	8 4+	
4	24 6+	6 3	6+	14+	
4 2	24 4+6	8 4+	6 3	21 3+	
5+	24 4+2	9+	7+	28 2+	
6+	24 2+12	9	8 4+		
6+3	24 12	12 3+	8 4		
6 3	28 2+	12 6	10+		
8+	28+7	15 3	10+2		
8 2+	28 2+14	18+2	12 3+		
8 4+	32+	18+	15+		
8 2	32 2+	18	15 3		
8	36 2+	21 3+	16 2+		
8 4	40 4+	24 6+	20 2+		
10+	40 2+	24 4+2	21 3+		
10+5	40 2+20	24 12	24 4+6		
11+	44+	27+	25+		
12+	48 2+	30 3+10	30+		
12 2+	52 2+	36+4	30 3+10		
12 3+	52 2+26	39 3+	35+		
12+3	56 4+14	42 3+7	40 4+		
12 2+6	60 2+	54+	50+		
12 2+2	60 2+5, 6, 30	57 3+			
12	60 6+10	60 6+10			
12 6	68 2+	84 3+			
16 2+	84 2+	93 3+			
16	84 2+6, 14, 21				
16+	88 2+				
20+	104 4+				
20 2+					

**Table 4.1.** Hauptmoduln with  $p$ -adic annihilation.

## 4 $p$ -adic annihilation

In this section, we restrict our focus to the  $n|h$ -type groups appearing in monstrous moonshine, and we prove the following theorem, first mentioned in the introduction, which gives a class of Hauptmoduln from monstrous moonshine that are  $p$ -adically annihilated for small primes  $p$ .

**Theorem 4.1.** *Let  $p$  be a prime. If  $\Gamma$  is an  $n|h$ -type group as specified in Table 4.1, then the Hauptmodul on  $\Gamma_\lambda$  is  $p$ -adically annihilated by  $U_p$ .*

For all Hauptmoduln  $\mathcal{T}$  appearing in monstrous moonshine, we computed  $\mathcal{T}|U_p^n$  for small values of  $n$  and small primes  $p$ . These data, as well as heuristics governing the sizes of the ordinary spaces  $\mathfrak{S}(\Gamma, [\lambda_t]_p)^0$  for  $n|h$ -type groups  $\Gamma$ , lead us to the following conjecture (the relevancy of the ordinary space to  $p$ -adic annihilation is discussed in Section 4.2).

**Conjecture 4.2.** *The converse to Theorem 4.1 holds, meaning that the Hauptmoduln of Table 4.1 are the only Hauptmoduln appearing in monstrous moonshine with  $p$ -adic annihilation. In particular, no Hauptmodul appearing in monstrous moonshine is  $p$ -adically annihilated for  $p \geq 13$ .*

**Remark 4.3.** Given an admissible  $n|h$ -type group  $\Gamma$ , we remark here on a method for showing  $\mathcal{T}_\Gamma$  is not  $p$ -adically annihilated for a given  $p$ . By Lemma 3.4, after applying  $U_p$  enough times we may assume that  $p \nmid nh$ . Then after further applying  $U_p$ , we have that  $\mathcal{T}|U_p^\alpha \in \tilde{M}_{p-1}(nh)$  for some  $\alpha$ . Since  $\tilde{M}_{p-1}(nh)$  is finite-dimensional, it is then straightforward to verify that  $\mathcal{T}$  is not  $p$ -adically annihilated. For small levels and primes, this method is easy to apply; for example one

finds that  $J$  is not 13-adically annihilated since  $J|U_{13}^2 \equiv J|U_{13} \pmod{13}$ . However, this method quickly starts requiring many coefficients of the Hauptmoduln and basis elements of  $M_{p-1}(nh)$ , particularly when  $p$  is large.

Empirically, it appears that for  $p=2, 3$  one may use a similar approach with the space  $\tilde{M}_4(nh)$ .

**Remark 4.4.** It is known that  $J|U_p \not\equiv 0 \pmod{p}$  for any  $p \geq 13$  [38], and see [16] for further study of such congruences.

In Section 4.1, generalizing formulas of Conway and Norton [10], we write down *compression formulas* which relate Hauptmoduln on different groups  $n|h$ -type groups appearing in Moonshine. These relations will reduce the verification of Theorem 4.1 to a smaller set of groups, which will be easier to verify computationally. In Section 4.2, we utilize the theory developed in Section 3 to prove annihilation for the entries in the table of Theorem 4.1 with  $p \geq 5$ . In Section 4.3, we use separate techniques due to Lehner and verify the remaining entries, corresponding to  $p = 2, 3$ . These techniques are sufficiently explicit to give rates of  $p$ -adic annihilation in certain cases. Finally, we discuss in Section 4.4 a connection between  $p$ -adic annihilation of Hauptmoduln and the group structure of the monster group.

### 4.1 Compression formulas

Throughout this section, we use the following notation. If  $\Gamma$  is the group  $\Gamma_0(n|h) + e_1, e_2, \dots$ , then we write  $\Gamma^d$  for the group  $\Gamma_0(n'|h') + e'_1, e'_2, \dots$  where  $n' = n/\gcd(n, d)$ ,  $h' = h/\gcd(h, d)$ , and  $e'_1, e'_2, \dots$  are the divisors of  $n'/h'$  among  $e_1, e_2, \dots$ . This notation comes from [10], where it is explained that for any element  $g$  of the monster, if  $\mathcal{T}_g$  is the Hauptmodul for the group  $\Gamma_\lambda$  corresponding to  $g$  from moonshine, then  $\mathcal{T}_{g^d}$  is the Hauptmodul for  $\Gamma_\lambda^d$ . Additionally, if  $\Gamma$  is the group  $\Gamma_0(n|h) + e_1, e_2, \dots$ , then we write  $\langle \Gamma, w_e \rangle$  for the group  $\Gamma_0(n|h) + e_1, e_2, \dots, e_1 * e, e_2 * e, \dots$  generated by  $\Gamma$  and  $w_e$ , if it exists. In this section, we will also adopt the notation  $\mathcal{T}_\Gamma$  for the Hauptmodul on  $\Gamma_\lambda$ .

The formula

$$p\mathcal{T}_\Gamma|U_p = \mathcal{T}_{\Gamma^p} - \mathcal{T}_\Gamma \quad \text{if } w_p \in \Gamma \tag{4.1}$$

relating the Hauptmodul for  $g^p$  with that of  $g$  for  $g \in \mathbb{M}$  appears in [10, Section 8]. The following relations are of a similar form, and they allow us to connect the  $p$ -adic properties of Hauptmoduln on closely related groups.

**Proposition 4.5.** *Let  $\Gamma$  be a  $p^r n|h$ -type group where  $p$  is prime and  $p \nmid nh$ . Then, whenever all of the relevant groups appear in monstrous moonshine,*

- (a)  $p\mathcal{T}_\Gamma|U_p = \mathcal{T}_\Gamma - \mathcal{T}_{\langle \Gamma, w_p \rangle}$  if  $r = 1$  and  $p \nmid e$  for  $w_e \in \Gamma$ ,
- (b)  $p^2\mathcal{T}_\Gamma|U_p^2 = \mathcal{T}_\Gamma - \mathcal{T}_{\Gamma^p}$  if  $r = 1$  and  $p \nmid e$  for  $w_e \in \Gamma$ ,
- (c)  $p\mathcal{T}_\Gamma|U_p = \mathcal{T}_{\langle \Gamma^p, w_{p^{r-1}} \rangle} - \mathcal{T}_{\Gamma^p}$  if  $r > 1$  and  $w_{p^r} \in \Gamma$ , and
- (d)  $\mathcal{T}_\Gamma|U_p = -\mathcal{T}_{\Gamma^p}|U_p$  if  $r = 2$  and  $w_{p^2} \in \Gamma$ .

**Remark 4.6.** If  $r = 1$ ,  $p \nmid e$  for  $w_e \in \Gamma$ , and  $\langle \Gamma, w_p \rangle$  appears in monstrous moonshine, then part (b) follows from part (a) and (4.1). However, part (b) holds even when  $\langle \Gamma, w_p \rangle$  is not admissible. For example  $4\mathcal{T}_{6|3}|U_2^2 = \mathcal{T}_{6|3} - \mathcal{T}_{3|3}$  even though  $6|3+$  is not admissible. Similarly, if  $r = 2$ ,  $w_{p^2} \in \Gamma$ , and  $\langle \Gamma^p, w_p \rangle$  appears in monstrous moonshine, then part (d) follows from parts (a) and (c), but part (d) holds even when  $\langle \Gamma^p, w_p \rangle$  is not admissible.

In each case, there are only finitely many Hauptmoduln satisfying the hypotheses, and for each, we may apply Lemma 2.9, use Sturm's bound, and check that sufficiently many of the

coefficients are zero (2500 coefficients suffice in all cases). These relations reduce the number of Hauptmoduln one needs to check to show that the Hauptmoduln in Theorem 4.1 are indeed annihilated. For example, (a) implies that if  $\Gamma$  is an  $pn|h$ -type group with  $p \nmid n$  and  $\mathcal{T}_\Gamma$  is  $p$ -adically annihilated, then so is  $\mathcal{T}_{\langle \Gamma, w_p \rangle}$ . Note that many of these formulas allow us to prove that  $\mathcal{T}_{\Gamma^p}$  is  $p$ -adically annihilated from the fact that  $\mathcal{T}_\Gamma$  is, which explains much of the structure in the figures in Appendix B. In some sense, Proposition 4.5 suggests that  $p$ -adic properties of Hauptmoduln must be closely related to moonshine modules, since they tend to be preserved under power maps in the underlying group. Since we have already proved that  $\mathcal{T}$  is  $p$ -adically annihilated in the cases where  $\mathcal{T}|U_p = 0$  (see Remark 2.5), we have altogether reduced the verification of Theorem 4.1 to the following much smaller check.

**Corollary 4.7.** *In order to show that the Hauptmoduln in Theorem 4.1 are  $p$ -adically annihilated, it suffices to check  $p$ -adic annihilation for the following smaller set shown in Table 4.2.*

2	3	5	7	11
6+3	6+2	4 2+	2+	3 3
6 3	24 4+2	6+	3 3	4 2+
10+5		6 3	4 2+	11+
22+11		7+	8 4+	
		8 4+		
		8 4		
		12 3+		
		16 2+		
		21 3+		
		24 4+6		
		30 3+10		

**Table 4.2.** Hauptmoduln for which it suffices to prove Theorem 4.1.

One has a significant amount of freedom in choosing these representatives – we have chosen those most conducive to performing computations when  $p = 2, 3$ . When  $p \geq 5$  we will prove Theorem 4.1 directly in Section 4.2 rather than using the reduction given here.

## 4.2 Annihilation via ordinary spaces

In this section, we will prove Theorem 4.1 for  $p \geq 5$  using the theory of  $p$ -adic modular forms developed in Section 3. The key observation relating the theory of  $p$ -adic modular forms to  $p$ -adic annihilation is the following easy consequence of Proposition 3.6.

**Lemma 4.8.** *Suppose that  $\mathfrak{S}(\Gamma, [\eta]_p)^0 \subseteq \mathbb{F}_p$ . If  $f$  is a weight 0  $p$ -adic modular form on  $(\Gamma, \eta)$ , we have  $f|U_p^n \rightarrow c$  in the  $p$ -adic limit, where  $c$  is the constant term of  $f$ .*

When  $f = \mathcal{T}|U_p$  for  $\mathcal{T}$  a Hauptmodul, then  $c = 0$ . By Lemma 3.4,  $f$  is a weight 0  $p$ -adic modular form on  $(\Gamma, \eta)$  for some  $\Gamma, \eta$ . Hence Lemma 4.8 applies.

Using the `mflashexpansion` and `mfatkin` functions in Pari [34], one can compute the actions of

$$x = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix},$$

and all Atkin–Lehner involutions on  $M_{p-1}(\Gamma, [\lambda_t]_p)$ . Then using elementary linear algebra, it is easy to find a basis for  $\mathfrak{S}(\Gamma, [\lambda]_p)^0 \subseteq M_{p-1}(\Gamma, [\lambda_t]_p)$ . We performed this computation for various  $n|h$  groups  $\Gamma$  appearing in monstrous moonshine with small values of  $n$  with  $p \nmid n$  (specifically,  $n \leq 24$  for  $p = 5$ ,  $n \leq 11$  for  $p = 7$ , and  $n \leq 7$  for  $p = 11$ ).

The  $\Gamma$  for which  $\mathfrak{S}(\Gamma, [\lambda]_p)^0 \subseteq \mathbb{F}_p$  are given in Table 4.3. Applying Lemma 3.4 to the Hauptmoduln of Table 4.1 then proves Theorem 4.1 for  $p \geq 5$ . We note that every group from Table 4.3 corresponds to at least one group from Theorem 4.1.

$p = 5$	1	2+	3+	3 3	4 2+	6+	6 3	7+	8 4+	8 4	12 3+	16 2+	24 4+6
$p = 7$	1	2+	3 3	4 2+	8 4+								
$p = 11$	1	3 3	4 2+										

**Table 4.3.**  $\Gamma$  such that  $\mathfrak{S}(\Gamma, [\lambda]_p)^0 \subset \mathbb{F}_p$ .

**Remark 4.9.** Another method for computing  $\mathfrak{S}(\Gamma, [\lambda]_p)$  is as follows. By drawing fundamental domains for  $\Gamma_{\lambda_t}$ , one can compute the dimension of the space  $M_{p-1}(\Gamma_{\lambda_t})$ . One then uses the  $q$ -expansions of the modular forms  $\mathcal{T}|U_p^m$  to compute a basis for  $\tilde{M}_{p-1}(\Gamma, [\lambda]_p)$ . Computing  $\mathfrak{S}(\Gamma, [\lambda]_p)^0$  then amounts to linear algebra. We carried out this procedure in Sage [36], giving an alternate verification of the results in Table 4.3. The Sturm’s bound calculations for this method require checking 3500 coefficients.

It is worth noting that these methods also apply to Hauptmoduln not appearing in monstrous moonshine. For example, if  $\Gamma = \Gamma_0(2|2)$  and  $\mathcal{T}$  is the Hauptmodul on  $\Gamma_\lambda$  then Lemma 3.4 gives that  $\mathcal{T}|U_5$  is a 5-adic modular form on  $(\Gamma, \lambda)$ . Using the method above, one can compute that  $\mathfrak{S}(\Gamma, [\lambda]_p)^0 = 0$ , so that  $\mathcal{T}$  is 5-adically annihilated.

Although the methods developed here do not directly give rates of annihilation, the following observation held in all cases from Table 4.3, when checked with 10000 coefficients.

**Remark 4.10.** Let  $\mathcal{T}$  be the Hauptmodul on some  $\Gamma_\lambda$  appearing in Table 4.1 for  $p \geq 5$ ,  $\Gamma'$  from Table 4.3 as given by Lemma 3.4, and  $\lambda'$  the corresponding eigenvalue map specified by Conway–Norton. Let  $m$  be the smallest integer such that  $U_p^m \tilde{M}_{p-1}(\Gamma', [\lambda']_p) = \mathfrak{S}(\Gamma', [\lambda']_p)^0$ . Numerically, we observe  $v_p(\mathcal{T}|U_p^{\ell+m+1}) \geq v_p(\mathcal{T}|U_p^\ell) + 1$ , bounding the rate of annihilation from below by  $1/(m + 1)$ . Moreover this choice of  $m$  appears to be tight. We pose the question of whether these observations continue to hold to in general.

### 4.3 Additional $p$ -adic annihilation

The ordinary spaces of Section 3.2 and the annihilation verified in Section 4.2 were restricted to  $p \geq 5$ . In this section, we use different techniques to explicitly verify  $p$ -adic annihilation for the six groups appearing in Corollary 4.7 for the primes  $p = 2, 3$ .

**Proposition 4.11.** *We have*

$$v_p(\mathcal{T}|U_p^n) \geq \lfloor n\alpha \rfloor,$$

when  $\mathcal{T}$  is the normalized Hauptmodul on  $\Gamma_\lambda$ , with parameters given in Table 4.4.

$\Gamma$	6+2	6+3	10+5	22+11	6 3	24 4+2
$p$	3	2	2	2	2	3
$\alpha$	3/2	1	3/2	1/2	3/2	1/2

**Table 4.4.** Rates of annihilation.

**Proof.** Throughout, we use  $\mathfrak{T}$  to denote the normalized Hauptmodul  $\mathcal{T}$  plus some constant, and  $\eta(\tau) = q^{1/24} \prod_{n \geq 1} (1 - q^n)$  is the *Dedekind eta function*. The constant will be specified by writing  $\mathfrak{T}$  as an eta-quotient given in [10] and recorded in Table 4.5. We follow the methods of [31, 32] for the  $j$ -function, and prove our six cases in parallel.

We first compute expansions of  $\mathfrak{T}$  at each cusp, and write  $\mathfrak{T}|U_p$  as a rational function in a Hauptmodul by subtracting off the principal part. Below, we write out the calculation for

$\Gamma$	6+2	6+3	10+5	22+11	6 3	24 4+2
$\mathfrak{T}$	$\frac{\eta(\tau)^4\eta(2\tau)^4}{\eta(3\tau)^4\eta(6\tau)^4}$	$\frac{\eta(\tau)^6\eta(3\tau)^6}{\eta(2\tau)^6\eta(6\tau)^6}$	$\frac{\eta(\tau)^4\eta(5\tau)^4}{\eta(2\tau)^4\eta(10\tau)^4}$	$\frac{\eta(\tau)^2\eta(11\tau)^2}{\eta(2\tau)^2\eta(22\tau)^2}$	$\frac{\eta(3\tau)^8}{\eta(6\tau)^8}$	$\frac{\eta(4\tau)\eta(8\tau)}{\eta(12\tau)\eta(24\tau)}$

**Table 4.5.** Eta quotients for unnormalized Hauptmoduln.

$p = 3$  and the group 6+2, and record only the formulas for the rest. These formulas may also be verified via a Sturm's bound coefficient check (600 suffice in all cases). Let

$$S_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & p \end{pmatrix} \quad \text{and} \quad F_2 = \begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix}.$$

For  $W_2$  a suitable Atkin–Lehner matrix on  $\Gamma_0(6)$ , we have

$$\begin{aligned} 3(\mathfrak{T}|U_3)(-1/2\tau) &= \sum_{\lambda=0}^2 \mathfrak{T}(S_\lambda F_2) = \mathfrak{T}(-1/6\tau) + \sum_{\lambda=1}^2 \mathfrak{T}(S_\lambda F_2\tau) \\ &= \mathfrak{T}(-1/6\tau) + \sum_{\mu=1}^2 \mathfrak{T}(W_2 T_\mu \tau) = \mathfrak{T}(-1/6\tau) + 3(\mathfrak{T}|U_3)(\tau) - \mathfrak{T}(\tau/3), \end{aligned}$$

and upon substituting  $\tau \mapsto 3\tau$  we obtain the cusp expansion

$$3(\mathfrak{T}|U_3)(-1/6\tau) = -q^{-1} + O(1).$$

We next subtract off this principal part with  $-\mathfrak{T}(\tau)$ . Sending  $\tau \mapsto -1/6\tau$  and applying the  $\eta$  functional equation to the quotients in Table 4.5, we find

$$3(\mathcal{T}|U_3)(\tau) = -3^4 \mathfrak{T}(\tau)^{-1} + c$$

for some constant  $c$ . One can check that  $\mathfrak{T}|U_p$  is bounded at the other cusps; see Lemma 2.4. For appropriate constants  $c$ , similar computations show

$$p(\mathcal{T}|U_p)(\tau) = -p^e \mathfrak{T}(\tau)^{-1} + c, \tag{4.2}$$

where  $e$  is as in Table 4.6.

$\Gamma$	6+2	6+3	10+5	22+11	6 3	24 4+2
$e$	4	6	4	2	4	1

**Table 4.6.** Parameters for functional equations.

These relations imply  $v_p(\mathcal{T}|U_p) \geq e - 1$ . Set  $Z = \mathfrak{T}^{-1}$  and  $W = p^e Z(\tau/p)$ . Expanding  $Z$  at other cusps and applying the principal part analysis as above, we find

$$p(p^e Z|U_p)(\tau) = f(p^e Z).$$

where  $f$  is a polynomial with  $f(\mathfrak{T}(\tau)) = \mathfrak{T}(p\tau) + O(q)$  (different for each group). Write

$$(Z|U_p)(\tau) = p^\alpha \sum_{j=1}^p b_j Z^j \tag{4.3}$$

where the coefficients  $b_j$  are listed in Table 4.7.

Following Lehner [32, equation (2.2)] gives

$$W^p + \sum_{j=1}^p (-1)^j p_j W^{p-j} = 0, \quad \text{where} \quad (-1)^{j+1} p_j = p^{e+\alpha+1} \sum_{m=j}^p b_m Z^{m-j+1}.$$



	6+2	6+3	10+5	22+11	6 3	24 4+2
$b_1$	$2 \cdot 3^{1/2}$	3	$2^{1/2}$	$2^{1/2}$	0	0
$b_2$	$4 \cdot 3^{5/2}$	$2^4$	$2^{3/2}$	$2^{1/2}$	$2^{3/2}$	0
$b_3$	$3^{11/2}$					$3^{1/2}$

**Table 4.7.** Polyomial coefficients.

This equation has roots  $W(\tau + \lambda)$  for  $\lambda \in \{0, \dots, p-1\}$ . If  $S_\ell$  denotes the sum of the  $\ell$ -th power of these roots, then we have  $p^{-e\ell-1}S_\ell = Z^\ell|U_p$ . We show that  $p^{\alpha(\ell-1)}(Z^\ell|U_p) \in p^\alpha Z \cdot \mathbb{Z}[p^\alpha Z, p^\alpha]$  for all  $\ell \geq 1$ . Equivalently, we check that  $S_\ell \in p^{(e-\alpha)\ell+1+\alpha}p^\alpha Z \cdot \mathbb{Z}[p^\alpha Z, p^\alpha]$ .

Lehner uses Newton sums to set up an induction, relating  $S_\ell$  to  $S_j$  for  $j < \ell$ . A similar computation works for our cases. The coefficients in Table 4.7 imply the base case  $\ell = 1$ . By Newton sums we have

$$S_\ell = \sum_{j=1}^{\ell} (-1)^{j+1} p_j S_{\ell-j},$$

where  $b_j, p_h = 0$  for  $j, h \geq p+1$  and  $S_0 = \ell$ . For  $\ell \leq p$  we rewrite the Newton sum as

$$S_\ell = \sum_{j=1}^{\ell-1} (-1)^{j+1} p_j S_{\ell-j} - (-1)^\ell \ell p_\ell.$$

By construction we have that  $p_j \in p^{e+1+\alpha+v_p(b_j)-\alpha}p^\alpha Z \cdot \mathbb{Z}[p^\alpha Z, p^\alpha]$  and applying the inductive hypothesis gives  $p_j S_{\ell-j} \in p^{e+1+\alpha+v_p(b_j)-\alpha+(e-\alpha)(\ell-j)+1+\alpha}p^\alpha Z \cdot \mathbb{Z}[p^\alpha Z]$ . We have the inequality  $e+1+\alpha+v_p(b_j)-\alpha \geq (e-\alpha)j$ , which one checks explicitly using the values of  $b_j$ . In particular,  $p_j S_{\ell-j} \in p^{(e-\alpha)\ell+1+\alpha}p^\alpha Z \cdot \mathbb{Z}[p^\alpha Z, p^\alpha]$ . We also check that  $\ell p_\ell \in p^{(e-\alpha)\ell+1+\alpha}p^\alpha Z \cdot \mathbb{Z}[p^\alpha Z, p^\alpha]$  from the explicit values of  $b_j$ . Thus  $S_\ell \in p^{(e-\alpha)\ell+1+\alpha}p^\alpha Z \cdot \mathbb{Z}[p^\alpha Z, p^\alpha]$  for  $\ell \leq p$ . When  $\ell \geq p+1$  we have

$$S_\ell = \sum_{j=1}^{\ell-1} (-1)^{j+1} p_j S_{\ell-j}$$

and we check that  $p_j S_{\ell-j} \in p^{(e-\alpha)\ell+1+\alpha}p^\alpha Z \cdot \mathbb{Z}[p^\alpha Z, p^\alpha]$  as above, which completes the induction. Thus, we have shown that

$$(p^{\alpha(\ell-1)} Z^\ell|U_p) \in p^\alpha Z \cdot \mathbb{Z}[p^\alpha Z, p^\alpha]$$

so that if  $g \in Z \cdot \mathbb{Z}[p^\alpha Z, p^\alpha]$ , then  $g|U_p \in p^\alpha Z \cdot \mathbb{Z}[p^\alpha Z, p^\alpha]$ . Note that  $\mathcal{T}|U_p = -p^{e-1}Z \in Z \cdot \mathbb{Z}[p^\alpha Z, p^\alpha]$ . Repeatedly applying the result of the induction thus gives the rates of annihilation claimed in Proposition 4.11. ■

**Remark 4.12.** These explicit techniques also apply when  $p \geq 5$ , as long as  $\mathcal{T}|U_p$  is modular on a genus zero group. For example, if  $\mathcal{T}$  is the Hauptmodul for 2+, then  $\mathcal{T}|U_5$  is modular on 10+2, which is genus zero. There are many examples for  $p \geq 5$  where this does not hold, e.g., if  $\mathcal{T}$  the Hauptmodul for 2+ then  $\mathcal{T}|U_7$  is modular on 14+2, which is genus one. For this example, the arguments of this section can be modified to obtain explicit lower bounds on the annihilation rate, e.g., by working with bivariate polynomials in appropriate meromorphic modular forms instead of single-variate polynomials in the Hauptmodul, since the latter do not exist for the genus one curve corresponding to 14+2. In general, however, we rely on the theory of Section 3 to prove  $p$ -adic annihilation as in Section 4.2.

#### 4.4 Preservation of annihilation under power maps

We discuss the relationship between Hauptmodul  $p$ -adic annihilation and power maps in the monster. We have already seen hints of this in Section 4.1. Unlike previous sections, this section will not be used elsewhere, except as motivation for Section 5.

**Definition 4.13.** For a fixed Hauptmodul  $\mathcal{T}_g$  and an integer  $d$ , we say that  $p$ -adic annihilation is *preserved under the  $d$ -th power map* if  $\mathcal{T}_g$   $p$ -adically annihilated implies  $\mathcal{T}_{g^d}$  is  $p$ -adically annihilated.

These relationships are depicted in Appendix B for primes  $p \leq 11$ , which we expect are the only primes with annihilation. Note that if  $d$  is relatively prime to the order of  $g$ , then  $\mathcal{T}_{g^d} = \mathcal{T}_g$ , so  $p$ -adic annihilation is preserved under the  $d$ -th power map. We will therefore restrict our attention to those  $d$  that divide the order of  $g$ . We first give conceptual explanations for this preservation of  $p$ -adic annihilation, when it holds. We then characterize exactly when  $p$ -adic annihilation is not preserved, and offer a notion of  $p$ -adic annihilation that seems to always be preserved under power maps. The average numerical rates of annihilation from Appendix A often do not decrease under power maps – we remark upon this briefly.

In certain situations, the compression formulas show that Hauptmodul  $p$ -adic annihilation is preserved under power maps, e.g. powering from the group  $\ell+$  to level 1, when  $\ell$  is prime. When  $p \geq 5$ , we may also explain via ordinary spaces.

**Example 4.14.** When  $p = 5$ , the groups  $50+$ ,  $10+2$ ,  $10+$ , and  $2+$  all have the same ordinary space  $\mathbb{F}_p = \mathfrak{S}(\Gamma_0(2)+, \mathbf{1})^0 \subseteq \tilde{M}_{p-1}(\Gamma_0(2)+, \mathbf{1}_t)$ , and their Hauptmoduln share the same annihilation behavior. This explains preservation of  $p$ -adic annihilation under  $p$ -th power maps. The compression formulas of Proposition 4.5 capture these same relations.

Furthermore, in light of Lemma 4.8 and Section 4.2, we seek inclusions of the form  $\mathfrak{S}(\Gamma^d, [\lambda]_p)^0 \hookrightarrow \mathfrak{S}(\Gamma, [\lambda]_p)^0$  for  $\Gamma$  being  $n|h$ -type with  $p \nmid nh$ . This would explain  $d$ -th power map preservation of  $p$ -adic annihilation from  $\Gamma_\lambda$  to  $\Gamma_\lambda^d$ , and similarly for groups with the same ordinary spaces. The following proposition accomplishes this in certain situations.

**Proposition 4.15.** *Let  $p \geq 5$  be prime,  $(d, nh) = 1$ ,  $\Gamma$  be an  $n|h$ -type group with eigenvalue map  $\eta$ , and  $\Gamma'$  be a  $dn|h$ -type group with eigenvalue map  $\eta'$  such that*

$$\text{AL}(\Gamma) = \text{AL}(\Gamma'), \quad (d, e) = 1 \quad \text{for all } e \in \text{AL}(\Gamma), \quad \text{and} \quad \eta|_{\Gamma'} = \eta'.$$

- (a) *There is an inclusion  $M_k(\Gamma, \eta) \subseteq M_k(\Gamma', \eta')$ .*
- (b) *For any  $\alpha \in \mathbb{Z}/(2p-2)\mathbb{Z}$ , there is an inclusion  $\mathfrak{S}(\Gamma, [\eta]_p)^\alpha \subseteq \mathfrak{S}(\Gamma', [\eta']_p)^\alpha$ .*

**Proof.** Part (b) follows from part (a) using the description of  $\mathfrak{S}$  given in the proof of Proposition 3.6. Part (a) follows from the isomorphic inclusion  $\Gamma/\Gamma_0(dnh) \hookrightarrow \Gamma'/\Gamma_0(nh)$  from Section 2.3. ■

**Remark 4.16.** Inclusions of the form  $M_k(\Gamma, \eta) \subseteq M_k(\Gamma', \eta')$  may have further implications for preserving average rates of  $p$ -adic annihilation via Remark 4.10.

We now discuss when power maps do not preserve Hauptmodul  $p$ -adic annihilation.

**Example 4.17.** If  $\mathcal{T}$  is the Hauptmodul on  $\Gamma_\lambda$  for  $\Gamma$  an  $n|h$ -type group, then the Hauptmodul on  $\Gamma_\lambda^d$  need not be annihilated when  $d \mid h$ , which describe all the grey boxes in the figures of Appendix B. For example, the Hauptmodul for  $6|3$  is 5-adically annihilated, but the Hauptmodul for 2 is not.

**Example 4.18.** If  $\mathcal{T}$  is the Hauptmodul on  $\Gamma_\lambda$  and  $\mathcal{T}|U_p = 0$ , power maps from  $\Gamma_\lambda$  may not preserve  $p$ -adic annihilation. For example, if  $\mathcal{T}$  is the Hauptmodul on 12,  $\mathcal{T}|U_p = 0$  while the Hauptmodul on 6 is not 2-adically annihilated.

The classes of groups from Examples 4.17 and 4.18 exhaust the situations for which power maps do not preserve Hauptmodul  $p$ -adic annihilation. If one further excludes the groups  $\Gamma$  with  $\mathcal{T}_\Gamma|U_p = 0$ , then rates of  $p$ -adic annihilation are preserved under power maps. These examples motivate a notion of strong  $p$ -adic annihilation for genus zero groups. This strong notion of annihilation will not be referenced outside of this section.

**Definition 4.19.** Let  $\Gamma$  be a genus zero group with Hauptmodul  $\mathcal{T}$ . We say that  $\Gamma$  has *strong  $p$ -adic annihilation* if every polynomial  $f(\mathcal{T})$  in the Hauptmodul with no constant term is  $p$ -adically annihilated.

In contrast with  $p$ -adic annihilation of Hauptmoduln, strong  $p$ -adic annihilation numerically appears to be always preserved under power maps. Furthermore, our numerical data indicate that rates of strong  $p$ -adic annihilation are also non-decreasing under power maps. We discussed polynomials in the Hauptmodul in Remark 3.5, and one finds that  $\Gamma_\eta$  has strong  $p$ -adic annihilation if  $\mathfrak{S}_{p-1}(\Gamma, \mathbf{1}_t)^0 = \mathbb{F}_p$  and  $\mathfrak{S}_{p-1}(\Gamma, [(\lambda^{\sigma_r})_t]_p)^0 = 0$  otherwise.

We can check that strong  $p$ -adic annihilation is now preserved for the groups of Example 4.17. Indeed, let  $\mathcal{T}$  be the Hauptmodul on  $\Gamma_\lambda$  for  $\Gamma$  an  $n|h$ -type group, and  $\mathcal{T}'$  be the Hauptmodul on  $\Gamma_\lambda^d$  for  $d | h$ . We recall the  $V_m$  operator, given by  $f|V_m = f \circ A$  where we set  $A = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$  as in Section 3.2. It acts on Fourier expansions by  $(\sum a(n)q^n)|V_m = \sum a(n)q^{mn}$ . From [10, Section 6], we know that  $\mathcal{T}'|V_d + c = \mathcal{T}^d$  for some constant  $c$ . In particular, if  $\mathcal{T}'$  is not  $p$ -adically annihilated,  $\mathcal{T}'|V_d$  is a polynomial in  $\mathcal{T}$  with no constant term and is also not  $p$ -adically annihilated. Thus, if  $\Gamma_\lambda^d$  does not have strong  $p$ -adic annihilation, neither does  $\Gamma_\lambda$ . This reflects the following inclusions.

**Proposition 4.20.** *Let  $p \geq 5$  and  $\Gamma$  be an  $n|h$ -type group with eigenvalue map  $\eta$ , and let  $\Gamma'$  be a  $nd|hd$  type group with eigenvalue map  $\eta'$  such that*

$$\begin{aligned} \text{AL}(\Gamma) &= \text{AL}(\Gamma'), & \eta'(x') &= \eta(x), & \eta'(y') &= \eta(y), & \text{and} \\ \eta'(W_e) &= \eta(W_e) & \text{for all } e &\in \text{AL}(\Gamma) \end{aligned}$$

for  $x, y$  and  $x', y'$  the usual generators of  $\Gamma_0(n|h)/\Gamma_0(nh)$  and  $\Gamma_0(nd|hd)/\Gamma_0(nhd^2)$ .

- (a) *There is an injection given by the operator  $V_d: M_k(\Gamma, \eta) \hookrightarrow M_k(\Gamma', \eta')$ .*
- (b) *For any  $\alpha \in \mathbb{Z}/(2p-2)\mathbb{Z}$ , this gives an injection  $V_d: \mathfrak{S}(\Gamma, [\eta]_p)^\alpha \hookrightarrow \mathfrak{S}(\Gamma', [\eta']_p)^\alpha$ .*

We observe empirically that strong  $p$ -adic annihilation is also preserved for the groups from Example 4.18, e.g.,  $\mathcal{T}^2$  is not 2-adically annihilated when  $\mathcal{T}$  is the Hauptmodul on 12.

Further aspects of this connection between  $p$ -adic properties of modular forms and the associated conjugacy classes of the monster group will be discussed in Section 5.

## 5 Moonshine

In this section, we will investigate groups with  $p$ -adic moonshine. Recall from the introduction that a *moonshine module* for a finite group  $G$  is a graded  $G$ -module  $V = \bigoplus_{n=-1}^\infty V_n$  such that

- (i) For each  $g \in G$ , the McKay–Thompson series

$$\mathcal{T}_g(\tau) = \sum_{n=-1}^\infty \text{Tr}(g|V_n)q^n$$

is the Hauptmodul of an order  $\text{ord}(g)$  conjugacy class of the monster.

- (ii) For any  $g \in G$  and any  $n \in \mathbb{Z}$ , if  $\mathcal{T}_g$  is the Hauptmodul for  $\Gamma$ , then  $\mathcal{T}_{g^n}$  is the Hauptmodul for  $\Gamma^n$ .

If for some prime  $p$ ,  $V$  also satisfies the following property, then we call  $V$  a *p-adic moonshine module*.

- (iii) For each irreducible character  $\chi$  of  $\Gamma$ , if  $m_\chi(n)$  is the multiplicity of  $\chi$  in the character of  $V_n$ , then the multiplicity generating function

$$\mathcal{M}_\chi(\tau) = \sum_{n=-1}^{\infty} m_\chi(n)q^n$$

associated to  $\chi$  is *p-adically annihilated*.

Throughout this section, we assume that Conjecture 4.2 holds. That is, we assume that Theorem 4.1 exactly characterizes which of the 171 Hauptmoduln appearing in monstrous moonshine are *p-adically annihilated* for each prime  $p$ .

We begin in Section 5.1 by stating basic facts about groups with *p-adic moonshine*, including the fact that for each prime  $p$ , only finitely many such groups exist. In Section 5.2, we illustrate *p-adic moonshine* with several examples of groups having *p-adic moonshine modules*. In Section 5.3, we find a surprising class of subgroups of the monster having *p-adic moonshine* in a slightly more general sense.

## 5.1 Basic facts

We begin by presenting an alternative formulation of *p-adic moonshine* that will allow us to make use of the results in Section 4.

**Lemma 5.1.** *Let  $G$  be a finite group with a moonshine module  $V = \bigoplus_{n=-1}^{\infty} V_n$ . For any prime  $p$ ,  $V$  is a *p-adic moonshine module* if and only if the McKay–Thompson series  $\mathcal{T}_g$  is *p-adically annihilated* for each  $g \in G$ .*

**Proof.** By the Schur orthogonality relations, we have

$$\mathcal{T}_g = \sum_{\chi \in \text{Irrep}(G)} \chi(g) \mathcal{M}_\chi \quad \text{for each } g \in G$$

and

$$\mathcal{M}_\chi = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \mathcal{T}_g \quad \text{for each } \chi \in \text{Irrep}(G).$$

If each  $\mathcal{M}_\chi$  is *p-adically annihilated*, then for all  $n \in \mathbb{N}$ , there exists  $N \in \mathbb{N}$  such that  $\mathcal{M}_\chi|U_p^N \equiv 0 \pmod{p^n}$ . Since each  $\chi(g)$  is an algebraic integer, it follows that  $\mathcal{T}_g|U_p^N \equiv 0 \pmod{p^n}$ , so each  $\mathcal{T}_g$  is *p-adically annihilated*. Similarly, if each  $\mathcal{T}_g$  is *p-adically annihilated*, then each  $|G|\mathcal{M}_\chi$ , and hence each  $\mathcal{M}_\chi$ , is also *p-adically annihilated*. ■

As an immediate consequence, a group  $G$  has *p-adic moonshine* if and only if we can assign to each element  $g \in G$  a *p-adically annihilated Hauptmodul*  $\mathcal{T}_g$  in a way that agrees with power maps in  $G$  and so that the multiplicities defined by

$$\mathcal{M}_\chi = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \mathcal{T}_g$$

have positive integral coefficients for all irreducible characters  $\chi$ . In particular, each McKay–Thompson series  $\mathcal{T}_g$  must be a Hauptmodul for one of the groups listed in Theorem 4.1. In fact, since we require that the assignment of group elements to Hauptmoduln agree with power maps, we can restrict our attention to only those congruence groups  $\Gamma$  with the property that  $\Gamma^n$  is  $p$ -adically annihilated for every  $n \in \mathbb{Z}$ . By Theorem 4.1, it follows that every McKay–Thompson series  $\mathcal{T}_g$  must be a Hauptmodul for one of the groups listed in Table 5.1.

	2	3	5	7	11
1	12 3+	1	1	1	1
2+	12+3	2+	2+	2+	3 3
2	12 6	3+	3+	3 3	11+
3+	16 2+	3	3 3	4 2+	
3 3	16	3 3	4 2+	7+	
4+	16+	6+	5+	7	
4 2+	20+	6+2	5	8 4+	
4	20 2+	9+	6+	14+	
4 2	20 2+5	9	7+	21 3+	
5+	22+	18+2	8 4+	28 2+	
6+	22+11	18+	10+		
6+3	24 2+	27+	10+2		
6 3	24+	54+	15+		
8+	24 2+3		15 3		
8 2+	24 6+		20 2+		
8 4+	24 12		21 3+		
8 2	32+		25+		
8	32 2+		30+		
8 4	40 4+		35+		
10+	40 2+		40 4+		
10+5	44+		50+		
11+	48 2+				
12+	88 2+				
12 2+					

**Table 5.1.** Candidate McKay–Thompson series for groups with  $p$ -adic moonshine.

As a first application of this simpler description of  $p$ -adic moonshine, the following proposition bounds the powers of primes dividing the orders of groups with  $p$ -adic moonshine for each prime  $p$ .

**Proposition 5.2.** *Let  $p$  be a prime and  $G$  be a group with  $p$ -adic moonshine. Assuming that Conjecture 4.2 holds, the following table gives for each prime  $q$  a value  $r$  such that every group  $G$  with  $p$ -adic moonshine satisfies  $v_q(|G|) \leq r$ .*

	$p = 2$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p > 11$
$q = 2$	46	12	15	15	0	0
$q = 3$	8	21	8	3	3	0
$q = 5$	3	0	9	0	0	0
$q = 7$	0	0	2	6	0	0
$q = 11$	2	0	0	0	2	0
$q > 11$	0	0	0	0	0	0

**Proof.** First, note that if  $q \mid |G|$ , then by Cauchy’s theorem,  $G$  contains an element of order  $q$ , so there must be some Hauptmodul corresponding to a  $q|h$ -type group in Table 5.1. This proves all of the cases with  $r = 0$  above.

For the remaining cases with  $r > 0$ , we follow the method given in [12]. Let  $J, \mathcal{T}_1, \dots, \mathcal{T}_n$  be the distinct Hauptmoduln given in Table 5.1 as candidate McKay–Thompson series for groups with  $p$ -adic moonshine. For each  $i \in \{1, \dots, n\}$ , let  $a_i$  be the number of elements of  $G$  whose McKay–Thompson series is  $\mathcal{T}_i$ . Then, the multiplicity of the trivial character  $\epsilon$  is

$$\mathcal{M}_\epsilon = \frac{1}{|G|} \sum_{g \in G} \mathcal{T}_g = \frac{1}{|G|} (J + a_1 \mathcal{T}_1 + \dots + a_n \mathcal{T}_n).$$

In particular, since  $\mathcal{M}_\epsilon$  must have integral coefficients, it follows that

$$J + a_1\mathcal{T}_1 + \cdots + a_n\mathcal{T}_n \equiv 0 \pmod{|G|}.$$

Therefore, if we choose  $r$  large enough so that there are no coefficients  $a_1, \dots, a_n$  such that

$$J + a_1\mathcal{T}_1 + \cdots + a_n\mathcal{T}_n \equiv 0 \pmod{q^{r+1}},$$

then we have shown that  $v_q(|G|) \leq r$ . As in [12], this computation was carried out using Sage [36] by computing the kernel of the matrix of coefficients of  $J, \mathcal{T}_1, \dots, \mathcal{T}_n$ . ■

## 5.2 Examples of groups with $p$ -adic moonshine

We begin by illustrating the process of showing a group has  $p$ -adic moonshine using the group  $A_5$  and the prime  $p = 5$ . The character table for  $A_5$  is given below:

$A_5$	1	(1 2)(3 4)	(1 2 3)	(1 2 3 4 5)	(1 3 4 5 2)
$\epsilon$	1	1	1	1	1
$\chi_1$	4	0	1	-1	-1
$\chi_2$	5	1	-1	0	0
$\chi_3$	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
$\chi_4$	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

**Table 5.2.** Character Table for  $A_5$ .

The square of any element of the fourth conjugacy class listed in the character table is in the fifth conjugacy class, so any moonshine module must have the same McKay–Thompson series for elements of those two conjugacy classes. The only other non-trivial power relations come from the fact that  $g^{\text{ord}(g)} = 1$  for any  $g$ , so a possible assignment of 5-adically annihilated McKay–Thompson series that agrees with power maps in  $A_5$  is given by assigning  $\mathcal{T}_1$  to the element of the conjugacy class of 1,  $\mathcal{T}_{2+}$  to the elements of the conjugacy class of (1 2)(3 4),  $\mathcal{T}_{3|3}$  to the elements of the conjugacy class of (1 2 3), and  $\mathcal{T}_5$  to the elements of the conjugacy classes of (1 2 3 4 5) and (1 3 4 5 2). The associated multiplicities are then given by

$$\begin{aligned} \mathcal{M}_\epsilon &= q^{-1} + 4378q + 382380q^2 + 14714988q^3 + 340105628q^4 + O(q^5), \\ \mathcal{M}_{\chi_1} &= 13122q + 1432996q^2 + 57620010q^3 + 1349723748q^4 + O(q^5), \\ \mathcal{M}_{\chi_2} &= 17500q + 1815128q^2 + 72334998q^3 + 1689829376q^4 + O(q^5), \\ \mathcal{M}_{\chi_3} &= 8753q + 1050626q^2 + 42904992q^3 + 1009618126q^4 + O(q^5), \quad \text{and} \\ \mathcal{M}_{\chi_4} &= 8753q + 1050626q^2 + 42904992q^3 + 1009618126q^4 + O(q^5). \end{aligned}$$

In order to show that this gives a valid moonshine module, we must show that these multiplicities are both positive and integral. For positivity, we may use inequality (4.16) in [12]. Indeed, this inequality holds for  $n = 2$ , and hence for all  $n \geq 2$  since the left-hand side is monotonically increasing. Since the first coefficients of each multiplicity generating function are positive, this implies that all of them must be. For integrality, we may simply note that each multiplicity generating function is on  $\Gamma_0(90)$ , so we may use Sturm’s bound to reduce the computation to checking only the coefficients up to  $q^{216}$ . Using Sage [36], it turns out to indeed be the case that all of the coefficients are integers. Thus,  $A_5$  has 5-adic moonshine with the McKay–Thompson series given above.

In fact, it turns out that  $p$ -adic moonshine is not such a rare phenomenon among groups with small orders. Indeed, using Sage [36], we have computed that for every prime  $p$ , every group  $G$

of order at most 25 for which there is some assignment of  $p$ -adically annihilated Hauptmoduln to elements of  $G$  obeying power maps has  $p$ -adic moonshine. In fact, out of all 45252 such feasible assignments, only 11 do not give rise to a  $p$ -adic moonshine module, and all 11 exceptions are for  $p = 2$  and the group  $G = \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2$ .

In certain special cases, these computations become somewhat simpler. For example, consider the case of a non-trivial group  $G$  in which we assign every non-identity element the same Hauptmodul  $\mathcal{T}$ . In particular, this means that every non-identity element of  $G$  must have order  $q$  for some prime  $q$ . We will characterize exactly when  $G$  has a  $p$ -adic moonshine module under this assignment.

Under such an assignment, the multiplicity of the trivial character  $\epsilon$  is given by

$$\mathcal{M}_\epsilon = \frac{1}{|G|} \sum_{g \in G} \mathcal{T}_g = \frac{1}{|G|}(J - \mathcal{T}) + \mathcal{T},$$

and the multiplicity of any non-trivial character  $\chi$  is given by

$$\mathcal{M}_\chi = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \mathcal{T}_g = \frac{1}{|G|} \left( \overline{\chi(e)} J + \sum_{g \in G - \{e\}} \overline{\chi(g)} \mathcal{T} \right) = \frac{\dim \chi}{|G|} (J - \mathcal{T}).$$

These multiplicities are both integral if and only if  $|G| \mid (J - \mathcal{T})$ , and for checking positivity, we may once again use inequality (4.16) in [12]. After a computation in Sage [36], we have the following result.

**Proposition 5.3.** *Let  $p$  and  $q$  be primes,  $G$  be a group of exponent  $q$ , and  $\mathcal{T}$  be a Hauptmodul for one of the order  $q$  conjugacy class of the monster. Then, assuming that Conjecture 4.2 holds,  $G$  has a  $p$ -adic moonshine module in which the McKay–Thompson series for each non-identity element is  $\mathcal{T}$  if and only if  $p$  and  $\mathcal{T}$  appear in the following table and  $|G| \leq q^r$  where  $r$  is the corresponding entry in the third row.*

$p$	2	2	2	3	3	3	5	5	7	7	11
$\mathcal{T}$	2+	2	3 3	3+	3	3 3	5+	5	7+	7	11+
$r$	12	13	1	6	9	3	3	5	2	4	2

### 5.3 Centralizers in the monster

Other examples of  $p$ -adic moonshine come from subgroups of the monster meeting only those conjugacy classes whose Hauptmoduln are  $p$ -adically annihilated, though Proposition 5.3 shows that not every group with  $p$ -adic moonshine is of this form. In this section, we will exhibit a surprising class of subgroups of the monster having  $p$ -adic moonshine in a slightly more general sense.

Specifically, we say that a modular function  $f$  is *weakly  $p$ -adically annihilated* if  $f|U_p^n \equiv 0 \pmod{p}$  for some  $n \geq 0$ , and that a moonshine module is a *weakly  $p$ -adic moonshine module* if each McKay–Thompson series is weakly  $p$ -adically annihilated. For  $p \geq 5$ , every McKay–Thompson series in monstrous moonshine that is weakly  $p$ -adically annihilated is also  $p$ -adically annihilated, so weakly  $p$ -adic moonshine and  $p$ -adic moonshine coincide. For  $p \in \{2, 3\}$ , however, these notions diverge. In addition to those in Table 4.1, the McKay–Thompson series given in Table 5.3 are weakly  $p$ -adically annihilated. In each case, this may be verified with a finite check using Sturm’s bound (with at most 3500 coefficients).

Using GAP [21], we have found that for each  $p \in 2, 3, 5, 7, 11$ , the centralizer of a  $pA$ -pure elementary abelian subgroup of the monster of order  $p^2$  has weakly  $p$ -adic moonshine given by restricting the monster module. The ATLAS names of these groups, which were found



2			3		
3	15+	30+	2	13+	28+
5	15+5	30+3, 5, 15	4+	14+	30+6, 10, 15
6+6	15 3	30+5, 6, 30	4 2+	14+7	30+
6+2	17+	30 3+10	4 2	15+	31+
6	18+	33+	5+	15+5	34+
7+	18+9	34+	5	15+15	36+
7	19+	35+	6+6	16 2+	36 2+
9+	20+4	36+	6+3	17+	39+
10+2	20+20	38+	6	18+9	40 4+
10+10	21+	41+	7+	18+18	40 2+
10	21+21	42+	8 2+	19+	42+
12+4	24+8	42+6, 14, 21	8 4	20 2+	45+
12+12	24+24	51+	10+	20 2+5	48 2+
13+	26+	56+	10+10	20 2+10	51+
13	26+26	60+	12+	21+	60 2+
14+	28+	66+	12+4	24 2+	60 2+5, 6, 30
14+7	29+	70+	12 2+	24 4+6	62+
14+14			12 2+6	26+	78+
			12 2+2	28 2+	84 2+

**Table 5.3.** Additional weakly  $p$ -adically annihilated McKay–Thompson series.

using [9, 42], are given in Table 5.4. In fact, each group in Table 5.4 intersects only those conjugacy classes whose Hauptmodul  $\mathcal{T}$  satisfy  $\mathcal{T}|U_p \equiv 0 \pmod{p}$ , which is somewhat stronger than weakly  $p$ -adic annihilation.

$p$	2	3	5	7	11
$C(pA^2)$	$2^2 \cdot {}^2E_6(2)$	$3^2 \times O_8^+(3)$	$5^2 \times U_3(5)$	$7^2 \times L_2(7)$	$11^2$
$\#C(pA^2)$	$2^{38} \cdot 3^9 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$2^{12} \cdot 3^{14} \cdot 5^2 \cdot 7 \cdot 13$	$2^4 \cdot 3^2 \cdot 5^5 \cdot 7$	$2^3 \cdot 3 \cdot 7^3$	$11^2$

**Table 5.4.** Subgroups of the monster with weakly  $p$ -adic moonshine.

In light of this, it is natural to ask whether there are other natural subgroups of the monster having  $p$ -adic or weakly  $p$ -adic moonshine and whether there is an explanation intrinsic to the monster for the existence of weakly  $p$ -adic moonshine for these subgroups. More generally, we pose the question of whether the results of this paper extend to other known cases of moonshine, such as Conway moonshine [15], umbral moonshine [14], and Thompson moonshine [24]. Do analogues of the groups in Table 5.4 exist for these other groups?

## A Table of annihilation

The following table gives the precise congruences that numerically appear to be satisfied by each Hauptmodul. The notation  $a_1, \dots, a_m \rightarrow b_1, \dots, b_n$  means the sequence beginning  $a_1, \dots, a_m$ , and then each subsequent term is given by adding  $b_k \pmod{n}$  from  $k = 1$  to  $\infty$ . For example,  $0, 1 \rightarrow 0, 3$  is the sequence  $0, 1, 1, 4, 4, 7, 7, 10, 10, \dots$ . The entry under  $p$  for the group  $\Gamma$  indicates the sequence  $a_1, a_2, a_3, \dots$  such that  $a_n$  is the highest power of  $p$  dividing  $\mathcal{T}_\Gamma|U_p^n$ . If no such cyclic pattern is clear, then we simply list the first few terms of the sequence in parentheses.

Class	Group	$p = 2$	$p = 3$	$p = 5$	$p = 7$	$p = 11$
1A	1	11 $\rightarrow$ 3	5 $\rightarrow$ 2	2 $\rightarrow$ 1	1 $\rightarrow$ 1	1 $\rightarrow$ 1
2A	2+	11 $\rightarrow$ 3	(3, 5, 9, 9, 11)	(1, 2, 3, 5, 5)	1 $\rightarrow$ 1	0 $\rightarrow$ 0
2B	2	11 $\rightarrow$ 3	1 $\rightarrow$ 0	0 $\rightarrow$ 0	0 $\rightarrow$ 0	0 $\rightarrow$ 0
3A	3+	5 $\rightarrow$ 1	5 $\rightarrow$ 2	(1, 2, 3, 5, 5)	0 $\rightarrow$ 0	0 $\rightarrow$ 0
3B	3	2 $\rightarrow$ 0	5 $\rightarrow$ 2	0 $\rightarrow$ 0	0 $\rightarrow$ 0	0 $\rightarrow$ 0
3C	3 3	3 $\rightarrow$ 3, 0	$\infty$	0 $\rightarrow$ 1, 0	1 $\rightarrow$ 1	0 $\rightarrow$ 1, 0
4A	4+	11 $\rightarrow$ 3	1 $\rightarrow$ 0	0 $\rightarrow$ 0	0 $\rightarrow$ 0	0 $\rightarrow$ 0
4B	4 2+	$\infty$	1 $\rightarrow$ 0	1 $\rightarrow$ 1	1 $\rightarrow$ 1	0 $\rightarrow$ 1, 0
4C	4	$\infty$	0 $\rightarrow$ 0	0 $\rightarrow$ 0	0 $\rightarrow$ 0	0 $\rightarrow$ 0
4D	4 2	$\infty$	1 $\rightarrow$ 0	0 $\rightarrow$ 0	0 $\rightarrow$ 0	0 $\rightarrow$ 0

5A	5+	$3 \rightarrow 2, 1, 3, 0$	$1 \rightarrow 0$	$2 \rightarrow 1$	$0 \rightarrow 0$	$0 \rightarrow 0$
5B	5	$1 \rightarrow 0$	$1 \rightarrow 0$	$2 \rightarrow 1$	$0 \rightarrow 0$	$0 \rightarrow 0$
6A	6+	$5 \rightarrow 1$	$(3, 5, 9, 9, 11)$	$1 \rightarrow 1$	$0 \rightarrow 0$	$0 \rightarrow 0$
6B	6+6	$2 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
6C	6+3	$5 \rightarrow 1$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
6D	6+2	$2 \rightarrow 0$	$(3, 5, 9, 9, 11)$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
6E	6	$2 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
6F	6 3	$3 \rightarrow 3, 0$	$\infty$	$0 \rightarrow 1, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
7A	7+	$2 \rightarrow 0$	$1 \rightarrow 0$	$1 \rightarrow 1$	$1 \rightarrow 1$	$0 \rightarrow 0$
7B	7	$2 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$1 \rightarrow 1$	$0 \rightarrow 0$
8A	8+	$7 \rightarrow 3$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
8B	8 2+	$\infty$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
8C	8 4+	$\infty$	$0 \rightarrow 1, 0$	$1 \rightarrow 1$	$0 \rightarrow 1, 0$	$0 \rightarrow 0$
8D	8 2	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
8E	8	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
8F	8 4	$\infty$	$1 \rightarrow 0$	$0 \rightarrow 1, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
9A	9+	$1 \rightarrow 0$	$5 \rightarrow 2$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
9B	9	$0 \rightarrow 0$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
10A	10+	$3 \rightarrow 2, 1, 3, 0$	$1 \rightarrow 0$	$(1, 2, 3, 5, 5)$	$0 \rightarrow 0$	$0 \rightarrow 0$
10B	10+5	$3 \rightarrow 2, 1, 3, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
10C	10+2	$1 \rightarrow 0$	$0 \rightarrow 0$	$(1, 2, 3, 5, 5)$	$0 \rightarrow 0$	$0 \rightarrow 0$
10D	10+10	$1 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
10E	10	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
11A	11+	$1 \rightarrow 1, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$1 \rightarrow 1$
12A	12+	$5 \rightarrow 1$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
12B	12+4	$2 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
12C	12 2+	$\infty$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
12D	12 3+	$3 \rightarrow 3, 0$	$\infty$	$0 \rightarrow 1, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
12E	12+3	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
12F	12 2+6	$\infty$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
12G	12 2+2	$\infty$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
12H	12+12	$2 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
12I	12	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
12J	12 6	$\infty$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
13A	13+	$2 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
13B	13	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
14A	14+	$2 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$1 \rightarrow 1$	$0 \rightarrow 0$
14B	14+7	$2 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
14C	14+14	$2 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
15A	15+	$1 \rightarrow 0$	$1 \rightarrow 0$	$(1, 2, 3, 5, 5)$	$0 \rightarrow 0$	$0 \rightarrow 0$
15B	15+5	$1 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
15C	15+15	$0 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
15D	15 3	$1 \rightarrow 0$	$\infty$	$0 \rightarrow 1, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
16A	16 2+	$\infty$	$0, 1 \rightarrow 0$	$0 \rightarrow 1, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
16B	16	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
16C	16+	$4, 6 \rightarrow 3$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
17A	17+	$1 \rightarrow 0$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
18A	18+2	$0 \rightarrow 0$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
18B	18+	$1 \rightarrow 0$	$(3, 5, 9, 9, 11)$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
18C	18+9	$1 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
18D	18	$0 \rightarrow 0$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
18E	18+18	$0 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
19A	19+	$1, 2 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
20A	20+	$3 \rightarrow 2, 1, 3, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
20B	20 2+	$\infty$	$1 \rightarrow 0$	$1 \rightarrow 1$	$0 \rightarrow 0$	$0 \rightarrow 0$
20C	20+4	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
20D	20 2+5	$\infty$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
20E	20 2+10	$\infty$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
20F	20+20	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
21A	21+	$1 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
21B	21+3	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
21C	21 3+	$0 \rightarrow 0$	$\infty$	$0 \rightarrow 1, 0$	$1 \rightarrow 1$	$0 \rightarrow 0$
21D	21+21	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
22A	22+	$1 \rightarrow 1, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
22B	22+11	$1 \rightarrow 1, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
23AB	23+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
24A	24 2+	$\infty$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
24B	24+	$3 \rightarrow 1$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
24C	24+8	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
24D	24 2+3	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
24E	24 6+	$\infty$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$

24F	24 4+6	$\infty$	$1 \rightarrow 0$	$(0, 0, 1, 2, 2)$	$0 \rightarrow 0$	$0 \rightarrow 0$
24G	24 4+2	$\infty$	$0 \rightarrow 1, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
24H	24 2+12	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
24I	24+24	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
24J	24 12	$\infty$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
25A	25+	$0 \rightarrow 0$	$0 \rightarrow 0$	$2 \rightarrow 1$	$0 \rightarrow 0$	$0 \rightarrow 0$
26A	26+	$2 \rightarrow 0$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
26B	26+26	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
27AB	27+	$0 \rightarrow 0$	$2 \rightarrow 2$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
28A	28 2+	$\infty$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$1 \rightarrow 1$	$0 \rightarrow 0$
28B	28+	$2 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
28C	28+7	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
28D	28 2+14	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
29A	29+	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
30A	30+6, 10, 15	$0 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
30B	30+	$1 \rightarrow 0$	$1 \rightarrow 0$	$1 \rightarrow 1$	$0 \rightarrow 0$	$0 \rightarrow 0$
30C	30+3, 5, 15	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
30D	30+5, 6, 30	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
30E	30 3+10	$1 \rightarrow 0$	$\infty$	$0 \rightarrow 1, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
30F	30+2, 15, 30	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
30G	30+15	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
31AB	31+	$0 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
32A	32+	$2, 3, 5 \rightarrow 3$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
32B	32 2+	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
33A	33+11	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
33B	33+	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
34A	34+	$1 \rightarrow 0$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
35A	35+	$1 \rightarrow 0$	$0 \rightarrow 0$	$1 \rightarrow 1$	$0 \rightarrow 0$	$0 \rightarrow 0$
35B	35+35	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
36A	36+	$1 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
36B	36+4	$0 \rightarrow 0$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
36C	36 2+	$\infty$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
36D	36+36	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
38A	38+	$1, 2 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
39A	39+	$0 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
39B	39 3+	$0 \rightarrow 0$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
39CD	39+39	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
40A	40 4+	$\infty$	$0, 1 \rightarrow 0$	$(1, 2, 3, 5, 5)$	$0 \rightarrow 0$	$0 \rightarrow 0$
40B	40 2+	$\infty$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
40CD	40 2+20	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
41A	41+	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
42A	42+	$1 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
42B	42+6, 14, 21	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
42C	42 3+7	$0 \rightarrow 0$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
42D	42+3, 14, 42	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
44AB	44+	$1 \rightarrow 1, 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
45A	45+	$0 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
46AB	46+23	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
46CD	46+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
47AB	47+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
48A	48 2+	$\infty$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
50A	50+	$0 \rightarrow 0$	$0 \rightarrow 0$	$(1, 2, 3, 5, 5)$	$0 \rightarrow 0$	$0 \rightarrow 0$
51A	51+	$1 \rightarrow 0$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
52A	52 2+	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
52B	52 2+26	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
54A	54+	$0 \rightarrow 0$	$(1, 2, 4, 8, 8)$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
55A	55+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
56A	56+	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
56BC	56 4+14	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
57A	57 3+	$0 \rightarrow 0$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
59AB	59+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
60A	60 2+	$\infty$	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
60B	60+	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
60C	60+4, 15, 60	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
60D	60+12, 15, 20	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
60E	60 2+5, 6, 30	$\infty$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
60F	60 6+10	$\infty$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
62AB	62+	$0 \rightarrow 0$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
66A	66+	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
66B	66+6, 11, 66	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
68A	68 2+	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$

69AB	69+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
70A	70+	$1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
70B	70+10, 14, 35	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
71AB	71+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
78A	78+	$0 \rightarrow 0$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
78BC	78+6, 26, 39	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
84A	84 2+	$\infty$	$0, 1 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
84B	84 2+6, 14, 21	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
84C	84 3+	$0 \rightarrow 0$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
87AB	87+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
88AB	88 2+	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
92AB	92+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
93AB	93 3+	$0 \rightarrow 0$	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
94AB	94+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
95AB	95+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
104AB	104 4+	$\infty$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
105A	105+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
110A	110+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$
119AB	119+	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$	$0 \rightarrow 0$

## B Power maps

For each  $p \in \{3, 5, 7, 11\}$  we record here the structure of the collection of groups whose Hauptmoduln are  $p$ -adically annihilated by  $U_p$  (the case  $p = 2$  appears as Fig. 1.1 in the introduction). In each diagram below, we write the groups  $\Gamma$  such that  $\mathcal{T}_\Gamma$  is  $p$ -adically annihilated by  $U_p$  but  $\mathcal{T}_\Gamma|_{U_p} \neq 0$ , and all of the powers of such groups. Solid lines indicate power maps, groups in white boxes satisfy  $\mathcal{T}_\Gamma|_{U_p} = 0$ , and groups in black boxes are not  $p$ -adically annihilated by  $U_p$  at all.

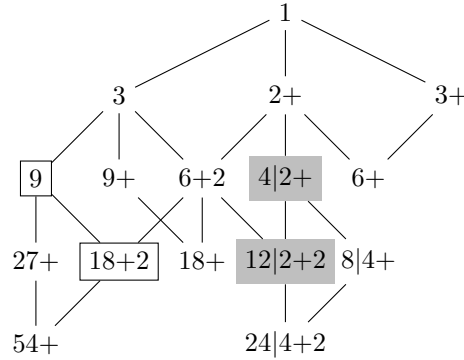


Figure B.1. Power maps for 3-adically annihilated Hauptmoduln.

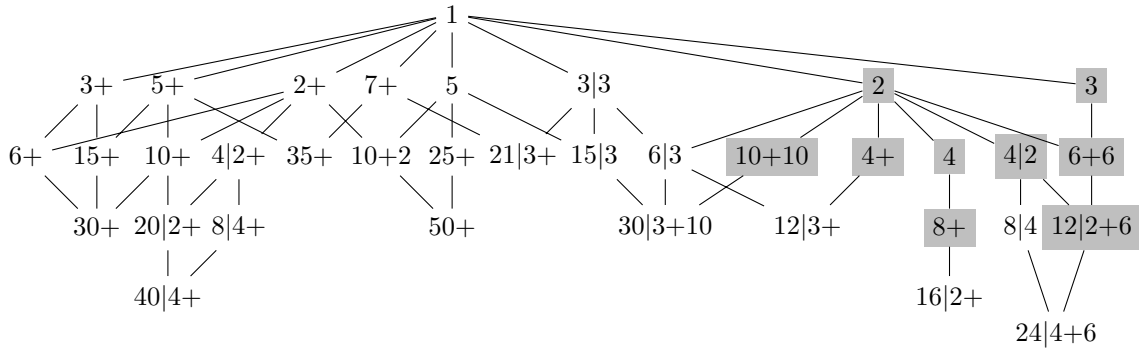
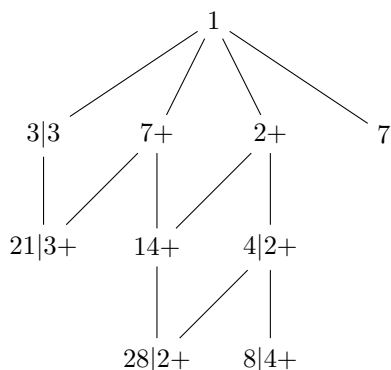
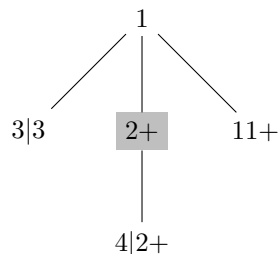


Figure B.2. Power maps for 5-adically annihilated Hauptmoduln.



**Figure B.3.** Power maps for 7-adically annihilated Hauptmodul



**Figure B.4.** Power maps for 11-adically annihilated Hauptmodul

## Acknowledgements

We wish to thank Ken Ono, John Duncan, and Larry Rolin for their support and guidance, as well as Frank Calegari for useful information regarding lifts of characteristic  $p$  modular forms for the primes  $p = 2, 3$ . We thank our referees for helpful comments. We also thank Emory University, Princeton University, the Asa Griggs Candler Fund, and NSF grant DMS-1557960.

## References

- [1] Andersen N., Jenkins P., Divisibility properties of coefficients of level  $p$  modular functions for genus zero primes, *Proc. Amer. Math. Soc.* **141** (2013), 41–53, [arXiv:1106.1188](https://arxiv.org/abs/1106.1188).
- [2] Atkin A.O.L., Proof of a conjecture of Ramanujan, *Glasgow Math. J.* **8** (1967), 14–32.
- [3] Atkin A.O.L., Lehner J., Hecke operators on  $\Gamma_0(m)$ , *Math. Ann.* **185** (1970), 134–160.
- [4] Borcherds R.E., Monstrous moonshine and monstrous Lie superalgebras, *Invent. Math.* **109** (1992), 405–444.
- [5] Borcherds R.E., Modular moonshine. III, *Duke Math. J.* **93** (1998), 129–154, [arXiv:math.QA/9801101](https://arxiv.org/abs/math/9801101).
- [6] Borcherds R.E., Ryba A.J.E., Modular moonshine. II, *Duke Math. J.* **83** (1996), 435–459.
- [7] Calegari F., Congruences between modular forms, available at <http://swc.math.arizona.edu/aws/2013/2013CalegariLectureNotes.pdf>.
- [8] Carnahan S., Generalized moonshine, IV: Monstrous Lie algebras, [arXiv:1208.6254](https://arxiv.org/abs/1208.6254).
- [9] Conway J.H., Curtis R.T., Norton S.P., Parker R.A., Wilson R.A., Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups, Oxford University Press, Eynsham, 1985.
- [10] Conway J.H., Norton S.P., Monstrous moonshine, *Bull. London Math. Soc.* **11** (1979), 308–339.
- [11] Conway J., McKay J., Sebbar A., On the discrete groups of Moonshine, *Proc. Amer. Math. Soc.* **132** (2004), 2233–2240.
- [12] DeHority S., Gonzalez X., Vafa N., Van Peski R., Moonshine for all finite groups, *Res. Math. Sci.* **5** (2018), 14, 34 pages, [arXiv:1707.05249](https://arxiv.org/abs/1707.05249).
- [13] Diamond F., Shurman J., A first course in modular forms, *Graduate Texts in Mathematics*, Vol. 228, Springer-Verlag, New York, 2005.
- [14] Duncan J.F.R., Griffin M.J., Ono K., Proof of the umbral moonshine conjecture, *Res. Math. Sci.* **2** (2015), 26, 47 pages, [arXiv:1503.01472](https://arxiv.org/abs/1503.01472).
- [15] Duncan J.F.R., Mack-Crane S., The moonshine module for Conway’s group, *Forum Math. Sigma* **3** (2015), e10, 52 pages, [arXiv:1409.3829](https://arxiv.org/abs/1409.3829).
- [16] Elkies N., Ono K., Yang T., Reduction of CM elliptic curves and modular function congruences, *Int. Math. Res. Not.* **2005** (2005), 2695–2707, [arXiv:math.NT/0512350](https://arxiv.org/abs/math.NT/0512350).
- [17] Ferenbaugh C.R., The genus-zero problem for  $n|h$ -type groups, *Duke Math. J.* **72** (1993), 31–63.

- [18] Frenkel I.B., Lepowsky J., Meurman A., A natural representation of the Fischer–Griess Monster with the modular function  $J$  as character, *Proc. Nat. Acad. Sci. USA* **81** (1984), 3256–3260.
- [19] Frenkel I.B., Lepowsky J., Meurman A., A moonshine module for the Monster, in Vertex Operators in Mathematics and Physics (Berkeley, Calif., 1983), *Math. Sci. Res. Inst. Publ.*, Vol. 3, Springer, New York, 1985 231–273.
- [20] Gannon T., Much ado about Mathieu, *Adv. Math.* **301** (2016), 322–358, [arXiv:1211.5531](https://arxiv.org/abs/1211.5531).
- [21] GAP – Groups, Algorithms, and Programming, Version 4.9.2, 2018, <https://www.gap-system.org>.
- [22] Gouvêa F.Q., Arithmetic of  $p$ -adic modular forms, *Lecture Notes in Mathematics*, Vol. 1304, Springer-Verlag, Berlin, 1988.
- [23] Harada K., Lang M.L., The McKay–Thompson series associated with the irreducible characters of the Monster, in Moonshine, the Monster, and Related Topics (South Hadley, MA, 1994), *Contemp. Math.*, Vol. 193, Amer. Math. Soc., Providence, RI, 1996, 93–111, [arXiv:q-alg/9412013](https://arxiv.org/abs/q-alg/9412013).
- [24] Harvey J.A., Rayhaun B.C., Traces of singular moduli and moonshine for the Thompson group, *Commun. Number Theory Phys.* **10** (2016), 23–62, [arXiv:1504.08179](https://arxiv.org/abs/1504.08179).
- [25] Hida H., Elementary theory of  $L$ -functions and Eisenstein series, *London Mathematical Society Student Texts*, Vol. 26, Cambridge University Press, Cambridge, 1993.
- [26] Jenkins P., Thornton D.J., Congruences for coefficients of modular functions, *Ramanujan J.* **38** (2015), 619–628, [arXiv:1404.0699](https://arxiv.org/abs/1404.0699).
- [27] Jochnowitz N., Congruences between systems of eigenvalues of modular forms, *Trans. Amer. Math. Soc.* **270** (1982), 269–285.
- [28] Katz N.M.,  $p$ -adic properties of modular schemes and modular forms, in Modular Functions of One Variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), *Lecture Notes in Math.*, Vol. 350, Editors W. Kuyk, J.-P. Serre, Springer, Berlin, 1973, 69–190.
- [29] Katz N.M., A result on modular forms in characteristic  $p$ , in Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), *Lecture Notes in Math.*, Vol. 601, Editors J.-P. Serre, D.B. Zagier, Springer, Berlin, 1977, 53–61.
- [30] Larson H., Coefficients of McKay–Thompson series and distributions of the moonshine module, *Proc. Amer. Math. Soc.* **144** (2016), 4183–4197, [arXiv:1508.03742](https://arxiv.org/abs/1508.03742).
- [31] Lehner J., Divisibility properties of the Fourier coefficients of the modular invariant  $j(\tau)$ , *Amer. J. Math.* **71** (1949), 136–148.
- [32] Lehner J., Further congruence properties of the Fourier coefficients of the modular invariant  $j(\tau)$ , *Amer. J. Math.* **71** (1949), 373–386.
- [33] Norton S.P., Generalized moonshine, in The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986), *Proc. Sympos. Pure Math.*, Vol. 47, Amer. Math. Soc., Providence, RI, 1987, 208–210.
- [34] Pari/GP (Version 2.11.0), University of Bordeaux, 2018, <http://pari.math.u-bordeaux.fr>.
- [35] Ryba A.J.E., Modular Moonshine?, in Moonshine, the Monster, and Related Topics (South Hadley, MA, 1994), *Contemp. Math.*, Vol. 193, Amer. Math. Soc., Providence, RI, 1996, 307–336.
- [36] SageMath, the Sage Mathematics Software System (Version 8.3), 2018, <http://www.sagemath.org>.
- [37] Serre J.-P., Formes modulaires et fonctions zêta  $p$ -adiques, in Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), *Lecture Notes in Math.*, Vol. 350, Editors W. Kuyk, J.-P. Serre, Springer, Berlin, 1973, 191–268.
- [38] Serre J.-P., Divisibilité de certaines fonctions arithmétiques, *Enseignement Math.* **22** (1976), 227–260.
- [39] Sturm J., On the congruence of modular forms, in Number Theory (New York, 1984–1985), *Lecture Notes in Math.*, Vol. 1240, Springer, Berlin, 1987, 275–280.
- [40] Thompson J.G., Finite groups and modular functions, *Bull. London Math. Soc.* **11** (1979), 347–351.
- [41] Thompson J.G., Some numerology between the Fischer–Griess Monster and the elliptic modular function, *Bull. London Math. Soc.* **11** (1979), 352–353.
- [42] Wilson R.A., The odd-local subgroups of the Monster, *J. Austral. Math. Soc. Ser. A* **44** (1988), 1–16.