TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY, SERIES B
Volume 9, Pages 1044–1064 (December 8, 2022)
https://doi.org/10.1090/btran/128

CONGRUENCES LIKE ATKIN'S FOR THE PARTITION FUNCTION

SCOTT AHLGREN, PATRICK B. ALLEN, AND SHIANG TANG

ABSTRACT. Let $p(n)$ be the ordinary partition function. In the 1960s Atkin found a number of examples of congruences of the form $p(Q^3\ell n+\beta)\equiv 0 \pmod{\ell}$ where ℓ and Q are prime and $5\leq \ell\leq 31$; these lie in two natural families distinguished by the square class of $1-24\beta \pmod{\ell}$. In recent decades much work has been done to understand congruences of the form $p(Q^m\ell n+\beta)\equiv 0 \pmod{\ell}$. It is now known that there are many such congruences when $m\geq 4$, that such congruences are scarce (if they exist at all) when $m=1,2$, and that for $m=0$ such congruences exist only when $\ell=5,7,11$. For congruences like Atkin's (when $m=3$), more examples have been found for $5\leq\ell\leq 31$ but little else seems to be known.

Here we use the theory of modular Galois representations to prove that for every prime $\ell\geq 5$, there are infinitely many congruences like Atkin's in the first natural family which he discovered and that for at least 17/24 of the primes ℓ there are infinitely many congruences in the second family.

1. Introduction

The partition function $p(n)$ counts the number of ways to write the positive integer n as the sum of a nonincreasing sequence of positive integers (by convention we agree that $p(0)=1$ and that $p(n)=0$ if $n\not\in\{0,1,2,\dots\}$). The study of the arithmetic properties of $p(n)$ has a long and rich history; interest in this topic stems not only from the fact that $p(n)$ is a fundamental function in additive number theory and combinatorics, but also from the fact that its generating function is a modular form of weight $-\frac{1}{2}$ on the full modular group.

The most famous examples of arithmetic phenomena for the partition function are the Ramanujan congruences

$$p(\ell n+\beta_\ell)\equiv 0 \pmod{\ell}\quad \text{for } \ell=5,7,11, \tag{1.1}$$

where $\beta_\ell := \frac{1}{24} \pmod{\ell}$. Extensions of these results for arbitrary powers of $5,7,11$ were conjectured and proved by Ramanujan, Watson and Atkin [Ram19, Ram20, Ram21, Wat38, Atk67]. On the other hand, after the work of the first author and Boylan [AB03] it is known that there are no congruences of the form (1.1) with $\ell\geq 13$.

Received by the editors December 17, 2021, and, in revised form, July 18, 2022.
2020 *Mathematics Subject Classification.* Primary 11F33, 11F80, 11P83.
The first author was supported by a grant from the Simons Foundation (#426145). The second author was supported by grants from the NSF (DMS-1902155) and NSERC. The third author was supported by a grant from the NSF (DMS-1902155).

Further examples of congruences for primes $\ell \leq 31$ were found by Newman, Atkin, and O'Brien [New57, AO67, Atk68]. These examples take the form

$$p(Q^m \ell n + \beta) \equiv 0 \pmod{\ell}, \tag{1.2}$$

where Q is a prime distinct from ℓ, and $m = 3$ or 4.

Many years later, Ono [Ono00] showed that for every $\ell \geq 5$, there are infinitely many primes Q for which we have a congruence (1.2) with $m = 4$. After the work of the first author and Ono [AO01a], we have the following (see [AO01b, Thm. 1]).

Theorem 1.1. *Suppose that $\ell \geq 5$ is prime and that $\left(\frac{1-24\beta}{\ell}\right) \in \{0, -1\}$. Then a positive proportion of primes $Q \equiv -1 \pmod{\ell}$ have the property that*

$$p\left(\frac{Q^3 n + 1}{24}\right) \equiv 0 \pmod{\ell} \qquad \text{if } Q \nmid n \ \text{ and } \ n \equiv 1 - 24\beta \pmod{\ell}. \tag{1.3}$$

For any such β, selecting n in one of $Q - 1$ residue classes modulo Q gives a congruence of the form

$$p(Q^4 \ell n + \beta') \equiv 0 \pmod{\ell} \tag{1.4}$$

with $\left(\frac{1-24\beta'}{\ell}\right) = \left(\frac{1-24\beta}{\ell}\right)$. Radu [Rad13] confirmed a conjecture of the first author and Ono by proving that if there is a congruence

$$p(mn + \beta) \equiv 0 \pmod{\ell} \quad \text{with } \ell \geq 5 \ \text{ prime},$$

then $\ell \mid m$ and $\left(\frac{1-24\beta}{\ell}\right) \in \{0, -1\}$.

After this discussion we know that there are many congruences of the form (1.2) with $m \geq 4$ and no congruences other than (1.1) with $m = 0$. It therefore becomes natural to ask about the existence of such congruences when $m = 1, 2, 3$.

Recent work of the first author, Beckwith and Raum [ABR] has shown that for $m = 1$ and $m = 2$, and for any prime $\ell \geq 5$, congruences of this form (if they exist at all) are extremely scarce in a precise sense. Since the main theorems of that paper require some notation to state, we mention here only Corollary 1.2: If $17 \leq \ell < 10000$ is prime, and S is the set of primes Q for which there is a congruence

$$p(Q\ell n + \beta) \equiv 0 \pmod{\ell},$$

then S has density zero.

This leaves open only the case $m = 3$, which is the focus of this paper. In this case, Atkin [Atk68] discovered many congruences of the form

$$p\left(Q^3 \ell n + \beta\right) \equiv 0 \pmod{\ell} \tag{1.5}$$

for small primes ℓ. These arise from two families which we describe in detail.

Let $13 \leq \ell \leq 31$ be prime. Atkin [Atk68, eq. (52)] gave examples of primes Q such that

$$p\left(\frac{Q^2 \ell n + 1}{24}\right) \equiv 0 \pmod{\ell} \ \text{ if } \ \left(\frac{n}{Q}\right) = \varepsilon_Q \tag{1.6}$$

for some $\varepsilon_Q \in \{\pm 1\}$. Fixing n in one of the allowable residue classes modulo Q produces a congruence of the form (1.5). For these small values of ℓ, the relevant generating functions are eigenforms of the Hecke operators, and Atkin's method relies on finding what he calls "accidental" eigenvalues (Atkin works with modular functions rather than modular forms, but the effect is the same). We will say that congruences (1.6) are of type "Atkin I."

Later, Weaver [Wea01] found more accidental eigenvalues for these primes (as well as more examples of congruences (1.3) with $\ell \mid n$). As an application of his performant algorithm to compute large values of the partition function, Johansson [Joh12] extended this list substantially; there are now more than 22 billion examples for primes $\ell \leq 31$.

For each of $\ell = 5, 7$ and 13, Atkin [Atk68, Thm. 1, 2] showed that if $Q \equiv -2 \pmod{\ell}$ then

$$p\left(\frac{Q^2n+1}{24}\right) \equiv 0 \pmod{\ell} \quad \text{if} \quad \left(\frac{-n}{\ell}\right) = -1 \quad \text{and} \quad \left(\frac{-n}{Q}\right) = -1. \tag{1.7}$$

We will say that congruences (1.7) are of type "Atkin II." To the authors' knowledge, no examples of such congruences are known for $\ell \geq 13$. After this discussion there are two natural questions:

(1) Are there congruences of type Atkin I for primes $\ell \geq 31$?
(2) Are there congruences of type Atkin II for primes $\ell \geq 13$?

We will refer to these congruences simply as "Type I" and "Type II" in what follows.

Remark. Once $\ell \geq 37$ the spaces of modular forms which are relevant for congruences of Type I are no longer one-dimensional. However, one may still perform a search for accidents in the sense of Atkin. For example, when $\ell = 37$, the relevant space is two-dimensional. A computation of the Hecke eigenvalues of the two newforms in this space for $Q < 10000$ yields three "accidents": there are three primes Q for which the Qth eigenvalue of each newform lies in the required residue class modulo a prime above ℓ in the field generated by its coefficients. In particular we have a congruence (1.6) when $Q = 6599$, 7541, and 9547. For example,

$$p\left(\frac{6599^2 \cdot 37n+1}{24}\right) \equiv 0 \pmod{37} \quad \text{if} \quad \left(\frac{n}{6599}\right) = -1,$$

which leads to 3299 congruences modulo 37 of the form (1.5) with $m = 3$. Similarly, we have

$$p\left(\frac{7541^2 \cdot 37n+1}{24}\right) \equiv 0 \pmod{37} \quad \text{if} \quad \left(\frac{n}{7541}\right) = 1.$$

Our goal in this paper is to prove that there are many congruences of the types which Atkin discovered. In particular we will prove the following theorems. (Note that for $\ell = 5, 7, 11$, the statements about congruences of Type I are trivially true in view of (1.1).)

The first result shows that congruences of Type I hold for every prime ℓ (an explicit description of what is meant by "positive proportion" is given at the end of this section).

Theorem 1.2. *Suppose that $\ell \geq 5$ is prime. Then a positive proportion of the primes $Q \equiv 1 \pmod{\ell}$ have the property that*

$$p\left(\frac{Q^2\ell n+1}{24}\right) \equiv 0 \pmod{\ell} \qquad \textit{if} \qquad \left(\frac{n}{Q}\right) = \left(\frac{-1}{Q}\right)^{\frac{\ell-3}{2}}.$$

The second result shows that for many primes ℓ we have congruences of Types I and II involving primes Q in a different residue class modulo ℓ.

Theorem 1.3. *Suppose that $\ell \geq 5$ is prime, and that*

$$\text{there exists an integer } a \text{ with } 2^a \equiv -1 \pmod{\ell}. \tag{1.8}$$

Then

(1) *A positive proportion of primes $Q \equiv -2 \pmod{\ell}$ have the property that for some $\varepsilon_Q \in \{\pm 1\}$, we have*
$$p\left(\frac{Q^2\ell n+1}{24}\right) \equiv 0 \pmod{\ell} \quad \text{if} \quad \left(\frac{n}{Q}\right) = \varepsilon_Q.$$
(2) *A positive proportion of primes $Q \equiv -2 \pmod{\ell}$ have the property that*
$$p\left(\frac{Q^2 n+1}{24}\right) \equiv 0 \pmod{\ell} \quad \text{if} \quad \left(\frac{-n}{\ell}\right) = -1 \quad \text{and} \quad \left(\frac{-n}{Q}\right) = -1.$$

Remark. By a result of Hasse [Has66], the proportion of primes ℓ for which (1.8) is satisfied is $17/24 \approx .708$.

Finally, we prove an analogous result under a similar assumption at the prime 3, although the situation here is slightly more complicated. We use the notation $S_k^{\text{new}}(6, \varepsilon_2, \varepsilon_3)$ to denote the new subspace of modular forms of integral weight k on $\Gamma_0(6)$ with eigenvalues ε_2 and ε_3 under the Atkin-Lehner involutions W_2 and W_3 (see the next section for details).

Theorem 1.4. *Suppose that $\ell \geq 5$ is prime, and that*

$$\text{there exists an integer } a \text{ with } 3^a \equiv -2 \pmod{\ell}. \tag{1.9}$$

Suppose further that there is no congruence modulo any prime above ℓ between distinct newforms in $S_{\ell-3}^{\text{new}}\left(6, -\left(\frac{8}{-\ell}\right), -\left(\frac{12}{-\ell}\right)\right)$. Then a positive proportion of primes $Q \equiv -2 \pmod{\ell}$ have the property that for some $\varepsilon_Q \in \{\pm 1\}$, we have
$$p\left(\frac{Q^2\ell n+1}{24}\right) \equiv 0 \pmod{\ell} \quad \text{if} \quad \left(\frac{n}{Q}\right) = \varepsilon_Q.$$
If (1.9) *holds and there is no congruence modulo any prime above ℓ between distinct newforms in $S_{\ell^2-3}^{\text{new}}(6, -1, -1)$ then a positive proportion of primes $Q \equiv -2 \pmod{\ell}$ have the property that*
$$p\left(\frac{Q^2 n+1}{24}\right) \equiv 0 \pmod{\ell} \quad \text{if} \quad \left(\frac{-n}{\ell}\right) = -1 \quad \text{and} \quad \left(\frac{-n}{Q}\right) = -1.$$

Remark. Approximately 82.8% of the primes $\ell < 100000$ satisfy either (1.8) or (1.9). For those which satisfy (1.9) but not (1.8) the additional hypothesis that there is no congruence between newforms is required due to a technical issue which is described in the last section. One expects that this condition should almost always be satisfied, and a computation shows that there is no congruence modulo any prime above ℓ between distinct newforms in $S_{\ell-3}^{\text{new}}\left(6, -\left(\frac{8}{-\ell}\right), -\left(\frac{12}{-\ell}\right)\right)$ for any $\ell < 150$.

However it seems very difficult to remove this condition. For example when $\ell = 71$, there is such a congruence between two newforms in the space $S_{\ell-3}^{\text{new}}\left(6, \left(\frac{8}{-\ell}\right), \left(\frac{12}{-\ell}\right)\right)$. In particular, this space contains a Galois orbit consisting of three newforms defined over a field which is ramified at 71, and this orbit gives rise to only two distinct reductions modulo the prime above 71.

To prove the existence of congruences (1.4), one must find primes Q for which the Hecke operator of index Q annihilates a suitable space of modular forms modulo some power of ℓ; the existence of such primes is guaranteed by a result of Serre [Ser76, ex. 6.4]. This approach extends to congruences modulo powers of ℓ [Ahl00, AO01a], and by work of Treneer [Tre06, Tre08] to a wide class of weakly holomorphic modular forms. The current situation is more delicate; we need to find primes Q for which the Hecke operator acts diagonally with a specified eigenvalue, which entails a much more careful study of the Galois representations which arise. In recent work, Raum [Rau21, Thm. E] has considered the converse question; given the existence of such a congruence as (1.4) or (1.5) he deduces information about the generalized Hecke eigenvalues λ_Q on a natural subspace of modular forms.

The Galois theoretic results which we prove may be of independent interest. Theorem 1.5 is the main theoretical input in the proof of Theorem 1.2 (here $S_k^{\mathrm{new}}(6)$ denotes the new subspace of cusp forms on $\Gamma_0(6)$ whose coefficients are integral at all primes above ℓ).

Theorem 1.5. *Suppose that m is a positive integer and that $\ell \geq 5$ is prime. Then a positive proportion of primes $Q \equiv 1 \pmod{\ell^m}$ have the following property: for every $g \in S_{\ell-3}^{\mathrm{new}}(6)$ we have*

$$g\big|T(Q) \equiv g \pmod{\ell^m}.$$

Above and in what follows, the positive proportion of primes appearing in our theorems is $\{2, 3, \ell\}$-Frobenian in the sense of [Ser12, §3.3] (we do not prove that the set of all primes satisfying the conclusions of our theorems is Frobenian, just that it contains a Frobenian subset). This means that there is a finite Galois extension $E/\mathbb{Q}$ unramified outside of $\{2, 3, \ell\}$ and a subset $C \subseteq \mathrm{Gal}(E/\mathbb{Q})$ that is a union of conjugacy classes such that the conclusion of the theorem holds for any prime Q with $\mathrm{Frob}_Q \in C$. We have not attempted to give a lower bound on the size of $|C|/|G|$, hence on the proportion of such primes Q, although in principle this is possible. We note the following subtlety. We first prove Theorem 1.5 under the further hypothesis that g is a newform, where the Frobenian set is more transparent, but modulo some possibly higher power $\ell^{m'}$ depending on how the lattice spanned by newforms sits inside of $S_{\ell-3}^{\mathrm{new}}(6)$ (see §2.3). The density of our Frobenian set depends on this m', hence on the relationship between these two lattices.

In the next section we give some background on modular forms and Galois representations. Section 3 is devoted to the proof of Theorem 1.5. The proof is technical, and most of the difficulty arises in establishing the result in the case $m = 1$. In Section 4 we use a different argument to prove two analogues of Theorem 1.5 in arbitrary weight; these results are the main input for the proofs of Theorems 1.3 and 1.4. The last section contains the proofs of the three main theorems.

2. Background

2.1. **Modular forms.** If f is a function on the upper half-plane, $k \in \frac{1}{2}\mathbb{Z}$, and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{Q})$, we define

$$\left(f\big|_k\gamma\right)(\tau) := (\det\gamma)^{\frac{k}{2}}(c\tau + d)^{-k} f(\gamma\tau).$$

Given $k \in \frac{1}{2}\mathbb{Z}$, a positive integer N, a multiplier system ν in weight k on $\Gamma_0(N)$, and a subring $A \subseteq \mathbb{C}$, we denote by $M_k(N, \nu, A)$, $S_k(N, \nu, A)$, and $M_k^!(N, \nu, A)$ the spaces of modular forms, cusp forms, and weakly holomorphic modular forms of weight k and multiplier ν on $\Gamma_0(N)$ whose Fourier coefficients lie in A. For basic properties of multiplier systems and modular forms one may consult for example [Kno70] and [DS05]. These forms satisfy the transformation law

$$f\big|_k\gamma = \nu(\gamma)f \quad \text{for} \quad \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$$

as well as the appropriate cusp conditions (weakly holomorphic forms are allowed poles at the cusps). If $\nu = 1$ we omit it from the notation. If in addition k is even, we let $S_k^{\mathrm{new}}(N, \mathbb{C}) \subseteq S_k(N, \mathbb{C})$ denote the new subspace, and define $S_k^{\mathrm{new}}(N, A) := S_k(N, A) \cap S_k^{\mathrm{new}}(N, \mathbb{C})$.

When N is square-free, there is an Atkin-Lehner involution W_p on $S_k(N, \mathbb{C})$ for every prime divisor p of N [AL70]. Given a tuple $\varepsilon = (\varepsilon_p)_{p|N}$ where each $\varepsilon_p \in \{\pm 1\}$, let $S_k^{\mathrm{new}}(N, \mathbb{C}, \varepsilon)$ be the subspace consisting of those forms f for which $f\big|_k W_p = \varepsilon_p f$ for each prime $p \mid N$.

Throughout, $\ell \geq 5$ will denote a fixed prime number. When A is the subring of algebraic numbers that are integral at all primes above ℓ, we omit it from the notation and simply write $M_k(N, \nu)$, $S_k(N, \nu)$, $M_k^!(N, \nu)$, and $S_k^{\mathrm{new}}(N)$. If in addition $\ell \nmid N$, then we write $S_k^{\mathrm{new}}(N, \varepsilon)$ for the subspace of $S_k^{\mathrm{new}}(N)$ attached to the tuple ε (this makes sense since for such ℓ, each involution W_p acts on $S_k^{\mathrm{new}}(N)$).

The Dedekind eta function is defined by

$$\eta(\tau) := q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n), \qquad q := e^{2\pi i \tau}.$$

Then the eta-multiplier ν_η is given by

$$\eta(\gamma\tau) = \nu_\eta(\gamma)(c\tau + d)^{\frac{1}{2}}\, \eta(\tau), \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

We collect some facts about modular forms which transform with a power of the eta-multiplier. Proofs for some of the nonobvious facts can be found in Section 2 of [ABR]. If $f \in M_k\left(1, \nu_\eta^r\right)$, then $\eta^{-r} f \in M_{k-\frac{r}{2}}^!(1)$. It follows that f has a Fourier expansion of the form

$$f = \sum_{n \equiv r\ (24)} a(n) q^{\frac{n}{24}}. \tag{2.1}$$

By (2.6) of [ABR] we have

$$M_k(1, \nu_\eta^r) = \{0\} \ \text{ unless } \ r \equiv 2k \pmod 4. \tag{2.2}$$

Let ν_θ be the multiplier on $\Gamma_0(4)$ attached to the theta function $\theta(\tau) = \sum q^{n^2}$ and define $f(\tau)\big|V_d := f(d\tau)$. By (2.7) of [ABR] and (2.2) we have

$$f \in M_k\left(1, \nu_\eta^r\right) \implies f\big|V_{24} \in M_k\left(576, \left(\frac{12}{\bullet}\right)\nu_\theta^r\right) = M_k\left(576, \left(\frac{12}{\bullet}\right)\nu_\theta^{2k}\right). \tag{2.3}$$

In particular $f\big|V_{24}$ is a modular form of half-integral weight in the sense of Shimura [Shi73].

For each prime $Q \geq 5$ we have the Hecke operator

$$T(Q^2) \,:\, S_k\left(1, \nu_\eta^r\right) \to S_k\left(1, \nu_\eta^r\right).$$

If $f \in S_k\left(1, \nu_\eta^r\right)$ with $(r, 24) = 1$ has Fourier expansion (2.1) then we have (see e.g. [Yan14, Proposition 11])

(2.4)
$$f\big|T(Q^2) = \sum \left(a(Q^2 n) + Q^{k-\frac{3}{2}} \left(\frac{-1}{Q}\right)^{k-\frac{1}{2}} \left(\frac{12n}{Q}\right) a(n) + Q^{2k-2} a\left(\frac{n}{Q^2}\right)\right) q^{\frac{n}{24}}.$$

For each squarefree t with $(t, 6) = 1$ there is a Shimura lift Sh_t on $S_k\left(1, \nu_\eta^r\right)$, defined via (2.3) and the Shimura lift [Shi73] on $S_k\left(576, \left(\frac{12}{\bullet}\right) \nu_\theta^{2k}\right)$. The action on Fourier expansions is given by

$$\mathrm{Sh}_t\left(\sum a(n) q^{\frac{n}{24}}\right) = \sum A_t(n) q^n,$$

where

$$A_t(n) = \sum_{d|n} \left(\frac{-1}{d}\right)^{k-\frac{1}{2}} \left(\frac{12t}{d}\right) d^{k-\frac{3}{2}}\, a\left(\frac{tn^2}{d^2}\right).$$

Then we have (see [ABR, (2.13)])

(2.5) $$f \equiv 0 \pmod{\ell} \iff \mathrm{Sh}_t(f) \equiv 0 \pmod{\ell} \qquad \text{for all squarefree } t.$$

From work of Yang [Yan14] it follows that we have

$$\mathrm{Sh}_t : S_k\left(1, \nu_\eta^r\right) \longrightarrow S_{2k-1}^{\mathrm{new}}\left(6, -\left(\frac{8}{r}\right), -\left(\frac{12}{r}\right)\right) \otimes \left(\frac{12}{\bullet}\right).$$

Moreover, for all primes $Q \geq 5$ we have

$$\mathrm{Sh}_t\left(f\big|T(Q^2)\right) = \left(\mathrm{Sh}_t f\right)\big|T(Q),$$

where $T(Q)$ is the Hecke operator of index Q on the integral weight space.

The connection with partitions is given by the fundamental relationship

$$\frac{1}{\eta(\tau)} = \sum p\left(\frac{n+1}{24}\right) q^{\frac{n}{24}}.$$

For our applications there are two important modular forms for each ℓ (see [ABR, §2] for the construction). In particular, there is a modular form $f_\ell \in S_{\frac{\ell-2}{2}}\left(1, \nu_\eta^{-\ell}, \mathbb{Z}\right)$ with

(2.6) $$f_\ell \equiv \sum p\left(\frac{\ell n+1}{24}\right) q^{\frac{n}{24}} \pmod{\ell}.$$

There is also a form $g_\ell \in S_{\frac{\ell^2-2}{2}}\left(1, \nu_\eta^{-1}, \mathbb{Z}\right)$ with

(2.7) $$g_\ell \equiv \sum_{\left(\frac{-n}{\ell}\right)=-1} p\left(\frac{n+1}{24}\right) q^{\frac{n}{24}} \pmod{\ell}.$$

From the discussion in Section 1, we have $g_\ell \not\equiv 0 \pmod{\ell}$, and

$$f_\ell \equiv 0 \pmod{\ell} \iff \ell = 5, 7, 11.$$

From the discussion above, each Shimura lift of f_ℓ is in the space

$$S_{\ell-3}^{\mathrm{new}}\left(6, -\left(\frac{8}{-\ell}\right), -\left(\frac{12}{-\ell}\right)\right) \otimes \left(\frac{12}{\bullet}\right),$$

and each Shimura lift of g_ℓ is in the space

$$S^{\mathrm{new}}_{\ell^2-3}(6,-1,-1)\otimes\left(\frac{12}{\bullet}\right). \tag{2.8}$$

2.2. **Modular Galois representations.** Let k and N be positive integers with k even and N coprime to ℓ. We recall properties of the Galois representations attached to eigenforms in $S_k(N)$ that will be used in the next section. We recall that $\ell \geq 5$.

We let $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. For each prime p, we fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and an embedding $\iota_p\colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Via ι_p, we view $G_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ as a subgroup of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We let $I_p \subseteq G_p$ denote the inertia subgroup and let $\mathrm{Frob}_p \in G_p/I_p$ denote the arithmetic Frobenius. We view the coefficients of any $f \in S_k(N)$ as elements of $\overline{\mathbb{Q}}_\ell$ via ι_ℓ.

We denote by $\chi\colon G_{\mathbb{Q}} \to \mathbb{Z}_\ell^\times$ (resp. $\omega\colon G_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$) the ℓ-adic (resp. the mod ℓ) cyclotomic character, and similarly with $G_{\mathbb{Q}}$ replaced by G_K for $K/\mathbb{Q}$ finite or by G_p with p a prime, etc. We let $\omega_2, \omega_2'\colon I_\ell \to \mathbb{F}_{\ell^2}^\times$ denote Serre's fundamental characters of level 2 [Ser87, §2.1]. These are characters of order ℓ^2-1 with $\omega_2^\ell = \omega_2'$, $\omega_2'^\ell = \omega_2$, and $\omega_2^{\ell+1} = \omega_2'^{\ell+1} = \omega$.

Theorem 2.1 summarizes some important properties of modular Galois representations, and is due to many people, including Deligne, Fontaine, Langlands, Ribet, and Shimura. See [Hid00, §3.2.2] and [Edi92, §2] for more details and references.

Theorem 2.1. *Let $f = q + \sum_{n\geq 2} a_n q^n \in S_k(N)$ be a normalized Hecke eigenform. There is a continuous irreducible representation $\rho_f\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ with semisimple mod ℓ reduction $\overline{\rho}_f\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ satisfying the following properties.*

(1) *If $p \nmid \ell N$, then ρ_f is unramified at p and the characteristic polynomial of $\rho_f(\mathrm{Frob}_p)$ is $X^2 - \iota_\ell(a_p)X + p^{k-1}$. This uniquely characterizes ρ_f. In particular, $\det\rho_f = \chi^{k-1}$.*
(2) *If $q \mid N$ and $q^2 \nmid N$, then $\rho_f|_{I_q}$ is unipotent. In particular, the prime-to-ℓ Artin conductor $N(\overline{\rho}_f)$ of $\overline{\rho}_f$ is not divisible by q^2. If further f is q-new, then $\rho_f|_{G_q}$ is an extension of ψ by $\chi\psi$ where $\psi\colon G_q \to \overline{\mathbb{Q}}_\ell^\times$ is the unramified character with $\psi(\mathrm{Frob}_q) = \iota_\ell(a_q)$.*
(3) *Assume that $2 \leq k \leq \ell+1$. Then*
   - *If $\iota_\ell(a_\ell)$ is an ℓ-adic unit, then $\rho_f|_{G_\ell}$ is reducible and $\rho_f|_{I_\ell}$ is an extension of the trivial character by χ^{k-1}.*
   - *If $\iota_\ell(a_\ell)$ is not an ℓ-adic unit, then $\overline{\rho}_f|_{G_\ell}$ is irreducible and $\overline{\rho}_f|_{I_\ell} \cong \omega_2^{k-1} \oplus \omega_2'^{(k-1)}$.*

Although we have suppressed it from the notation, we note that the representations ρ_f and $\overline{\rho}_f$ do depend on the choice of embedding $\iota_\ell\colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$, at least up to the prime that it determines in the coefficient field $\mathbb{Q}(\{a_n\}_{n\geq 1}) \subseteq \overline{\mathbb{Q}}$ of f.

2.3. **Congruences for non-eigenforms.** We will ultimately be interested in congruences for cusp forms which are not necessarily eigenforms. To do so, we record two lemmas which allow us to bootstrap from the case of newforms to the general case.

Let k and N be positive integers with k even and N coprime to ℓ. Let $f_1, \ldots, f_n \in S_k^{\mathrm{new}}(N)$ and write

$$f_j = \sum_{i=1}^{d} c_{i,j} g_i,$$

with newforms $g_1, \ldots, g_d \in S_k^{\mathrm{new}}(N)$ and $c_{i,j} \in \overline{\mathbb{Q}}$. Let E be a number field which contains the coefficients of each g_i as well as all of the coefficients $c_{i,j}$. Fix a prime λ of E over ℓ and let e be its ramification index. Define

$$m(f_1, \ldots, f_n) := \max(0, -\min(\mathrm{ord}_\lambda(c_{i,j}))). \tag{2.9}$$

With this notation we have the following.

Lemma 2.2. *Let the notation be as above and let $m \geq 1$ be an integer. Assume that there is a prime $Q \nmid N\ell$, an integer a, and an integer $r \geq 1$ such that $g_i \big| T(Q) \equiv a g_i \bmod \lambda^r$ for each $1 \leq i \leq d$. If $r \geq m + m(f_1, \ldots, f_n)$, then for $1 \leq j \leq n$ we have*

$$f_j \big| T(Q) \equiv a f_j \mod \lambda^m.$$

If further $f_1, \ldots, f_n \in S_k^{\mathrm{new}}(N, \mathbb{Z})$ and $r \geq em + m(f_1, \ldots, f_n)$ then for $1 \leq j \leq n$ we have

$$f_j \big| T(Q) \equiv a f_j \pmod{\ell^m}.$$

Proof. This follows immediately from the definitions of $m(f_1, \ldots, f_n)$ and ramification index. □

Lemma 2.3. *Let $m \geq 1$ be an integer. Let $Q \nmid N\ell$ be prime, let a be an integer, and let $r \geq 1$ be an integer such that $g_i \big| T(Q) \equiv a g_i \bmod \lambda^r$ for every newform $g \in S_k^{\mathrm{new}}(N)$. There is an integer $c \geq 0$, depending on ℓ, k, and N but not on Q, a, or m, such that if $r \geq em + c$, then*

$$f \big| T(Q) \equiv a f \pmod{\ell^m}$$

for all $f \in S_k^{\mathrm{new}}(N)$.

Proof. Let $A \subset \overline{\mathbb{Q}}$ be the subring of elements that are integral at all primes above ℓ (so $S_k^{\mathrm{new}}(N) = S_k^{\mathrm{new}}(N, A)$). Let $h_1, \ldots, h_d$ generate $S_k^{\mathrm{new}}(N)$ over A and let $f_1, \ldots, f_n$ be a basis for $S_k^{\mathrm{new}}(N, \mathbb{Z})$ (in fact we can take $n = d$). Since $S_k^{\mathrm{new}}(N, \mathbb{Z})$ generates $S_k^{\mathrm{new}}(N, \overline{\mathbb{Q}})$ over $\overline{\mathbb{Q}}$, we can write

$$h_j = \sum_{i=1}^{n} d_{i,j} f_i,$$

with $d_{i,j} \in \overline{\mathbb{Q}}$. Choose $c_0 \geq 0$ such that $\ell^{c_0} d_{i,j} \in A$ for each i, j. To show that $f \big| T(Q) \equiv af \pmod{\ell^m}$ for all $f \in S_k^{\mathrm{new}}(N)$, it suffices to show that $f_i \big| T(Q) \equiv a f_i \pmod{\ell^{m+c_0}}$ for each $1 \leq i \leq n$. Setting $c = ec_0 + m(f_1, \ldots, f_n)$ with $m(f_1, \ldots, f_n)$ as in (2.9), the lemma now follows from Lemma 2.2. □

Remark. When N is squarefree, the same result as Lemma 2.3 holds, replacing $S_k^{\mathrm{new}}(N)$ with $S_k^{\mathrm{new}}(N, \varepsilon)$.

3. Congruences in low weight

In this section, we use Galois representations together with some group theoretic arguments to prove Theorem 1.5, which implies Theorem 1.2. The proof is by induction with the bulk of the work devoted to proving the base case, which is essentially the combination of Propositions 3.3 and 3.8. A key technical lemma is Lemma 3.7, which roughly states that the mod ℓ Galois representations associated to sufficiently distinct normalized eigenforms cut out sufficiently disjoint field extensions. This lemma and its proof are inspired by and similar to that of [ACC$^+$, Lemma 7.1.5(3)].

We recall the standing assumption that $\ell \geq 5$ is prime. We again let k and N be positive integers with k even and N coprime to ℓ, and further assume that N is squarefree. Recall that we have a fixed embedding $\iota_\ell\colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ that allows us to view Fourier coefficients of modular forms in $S_k(N)$ as elements of $\overline{\mathbb{Q}}_\ell$.

Lemmas 3.1 and 3.2 are consequences of Theorem 2.1 and give us information on the image of the mod ℓ Galois representation associated to a normalized eigenform in $S_k(N)$.

Lemma 3.1. *Let $f, g \in S_k(N)$ be normalized eigenforms such that $\overline{\rho}_g \cong \overline{\rho}_f \otimes \eta$ for some nontrivial continuous character $\eta\colon G_\mathbb{Q} \to \overline{\mathbb{F}}_\ell^\times$. Then*

1. $\eta = \omega^{\frac{\ell-1}{2}}$.
2. *Assume further that $k \leq \ell - 1$. Letting a_ℓ denote the ℓ-th Fourier coefficient of f, we have*
   - *If $\iota_\ell(a_\ell)$ is an ℓ-adic unit, then $k = \frac{\ell+1}{2}$.*
   - *If $\iota_\ell(a_\ell)$ is not an ℓ-adic unit, then $k = \frac{\ell+3}{2}$.*

Proof. To prove that $\eta = \omega^i$ for some $1 \leq i \leq \ell - 2$, it suffices to show that η is unramified outside of ℓ. Take any prime $p \neq \ell$. Since we are assuming that N is squarefree, parts (1) and (2) of Theorem 2.1 imply that

$$\overline{\rho}_f|_{I_p} \cong \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix},$$

and similarly for $\overline{\rho}_g|_{I_p}$. Since $\overline{\rho}_g \cong \overline{\rho}_f \otimes \eta$, we must have $\eta|_{I_p} = 1$. To see that $i = \frac{\ell-1}{2}$, we use that

$$\det \overline{\rho}_f = \omega^{k-1} = \det \overline{\rho}_g = \eta^2 \det \overline{\rho}_f,$$

so $\eta = \omega^i$ is quadratic.

For part (2), we use part (3) of Theorem 2.1. If $\iota_\ell(a_\ell)$ is an ℓ-adic unit, it implies that $\omega^{k-1} = \omega^{\frac{\ell-1}{2}}$, so $k = \frac{\ell+1}{2}$. If $\iota_\ell(a_\ell)$ is not an ℓ-adic unit, it implies that

$$\omega_2^{k-1} = (\omega_2')^{k-1}\omega^{\frac{\ell-1}{2}} = \omega_2^{\ell(k-1)+\frac{\ell^2-1}{2}}.$$

Since ω_2 has order $\ell^2 - 1$, we obtain $k = \frac{\ell+3}{2}$. $\square$

Lemma 3.2. *Let $f = q + \sum_{n \geq 2} a_n q^n \in S_k(N)$ be a normalized eigenform. Assume that $2 \leq k \leq \ell - 1$ and that there is a prime $q \mid N$ such that f is q-new and $q^{k-1} \not\equiv q^{\pm 1} \pmod{\ell}$. Then the following are true.*

1. *$\overline{\rho}_f$ is irreducible.*
2. *Assume there is a quadratic extension $K/\mathbb{Q}$ such that $\overline{\rho}_f|_{G_K}$ is reducible. Then $\overline{\rho}_f \cong \overline{\rho}_f \otimes \omega^{\frac{\ell-1}{2}}$ and*
   - *If $\iota_\ell(a_\ell)$ is an ℓ-adic unit, then $k = \frac{\ell+1}{2}$.*

- *If $\iota_\ell(a_\ell)$ is not an ℓ-adic unit, then $k = \frac{\ell+3}{2}$.*

Proof. To establish part (1), assume that $\overline{\rho}_f \cong \psi_1 \oplus \psi_2$ for characters $\psi_i \colon G_\mathbb{Q} \to \overline{\mathbb{F}}_\ell^\times$. Since N is squarefree, $N(\overline{\rho}_f) \mid N$ is also squarefree and for every prime $p \neq \ell$, at most one of ψ_1, ψ_2 is ramified at p (see [Car89, §1.1], for example). On the other hand, $\det \overline{\rho}_f = \omega^{k-1}$, so $\psi_1\psi_2$ is unramified at all primes $p \neq \ell$. It follows that $\psi_1 = \omega^a$ and $\psi_2 = \omega^b$ for some $0 \leq a, b \leq \ell - 2$. Reordering if necessary, part (3) of Theorem 2.1 implies that $\psi_1 = \omega^{k-1}$ and $\psi_2 = 1$. This together with our assumption on q contradicts part (2) of Theorem 2.1.

We turn to part (2). Since $\overline{\rho}_f$ is irreducible we must have $\overline{\rho}_f|_{G_K} \cong \psi_1 \oplus \psi_2$ for nontrivial characters $\psi_1, \psi_2 \colon G_K \to \overline{\mathbb{F}}_\ell^\times$ which are permuted by $\mathrm{Gal}(K/\mathbb{Q})$. It follows that $\overline{\rho}_f$ is the induction of a character $\psi \colon G_K \to \overline{\mathbb{F}}_\ell^\times$ and letting η be the quadratic character of $K/\mathbb{Q}$, that $\overline{\rho}_f \cong \overline{\rho}_f \otimes \eta$. We then apply part (2) of Lemma 3.1. ∎

We apply Lemmas 3.1 and 3.2 to our particular space of interest $S_{\ell-3}^{\mathrm{new}}(6)$.

Proposition 3.3. *Recall that $\ell \geq 5$. For any newform $f \in S_{\ell-3}^{\mathrm{new}}(6)$, the image of $\overline{\rho}_f$ contains a conjugate of $\mathrm{SL}_2(\mathbb{F}_\ell)$.*

Proof. We first note that $S_2(6) = \{0\}$, so we may assume that $\ell \geq 7$.

By [DDT97, Theorem 2.47(b)], there are four possibilities for the image of $\overline{\rho}_f$:

(1) $\overline{\rho}_f$ is reducible.
(2) $\overline{\rho}_f$ is dihedral, i.e. $\overline{\rho}_f$ is irreducible but $\overline{\rho}_f|_{G_K}$ is reducible for some quadratic $K/\mathbb{Q}$.
(3) $\overline{\rho}_f$ is exceptional, i.e. the projective image of $\overline{\rho}_f$ is conjugate to one of A_4, S_4, or A_5.
(4) The image of $\overline{\rho}_f$ contains a conjugate of $\mathrm{SL}_2(\mathbb{F}_\ell)$.

We rule out each of the first three possibilities in turn.

First, $2^{\ell-4} \not\equiv 2^{\pm 1} \pmod{\ell}$ for any $\ell \geq 7$, so part (1) of Lemma 3.2 shows that $\overline{\rho}_f$ is irreducible. If further $\ell \geq 11$, then $\ell - 3 \neq \frac{\ell+1}{2}, \frac{\ell+3}{2}$, so part (2) of Lemma 3.2 shows that $\overline{\rho}_f$ is not dihedral. For $\ell = 7$, the space $S_4^{\mathrm{new}}(6)$ is one-dimensional and spanned by the newform

$$f = q - 2q^2 - 3q^3 + 4q^4 + 6q^5 + 6q^6 - 16q^7 + \cdots \tag{3.1}$$

by [LMF20]. If $\overline{\rho}_f$ were dihedral, then part (2) of Lemma 3.2 would imply that $\overline{\rho}_f \cong \overline{\rho}_f \otimes \omega^3$. Since $\omega^3(\mathrm{Frob}_5) = -1$, this would imply that $\mathrm{tr}\, \overline{\rho}_f(\mathrm{Frob}_5) = 0$. But $a_5 = 6 \not\equiv 0 \pmod{7}$, a contradiction.

It remains to rule out the exceptional case, and for this it suffices to show that the projective image contains an element of order ≥ 6. Since the characters ω and (ω_2/ω_2') have orders $\ell - 1$ and $\ell + 1$, respectively, the description of $\overline{\rho}_f|_{I_\ell}$ in part (3) of Theorem 2.1 implies that the projective image of $\overline{\rho}_f$ contains an element of order $\frac{\ell-1}{\gcd\{\ell-1,\ell-4\}}$ if $\iota_\ell(a_\ell)$ is a unit, and an element of order $\frac{\ell+1}{\gcd\{\ell+1,\ell-4\}}$ if $\iota_\ell(a_\ell)$ is not a unit. These are both ≥ 6 if $\ell = 11$, 17, or $\ell \geq 23$. When $\ell = 19$, there are three newforms in $S_{16}^{\mathrm{new}}(6)$ with LMFDB labels 6.16.a.a, 6.16.a.b, and 6.16.a.c. The values of a_ℓ for these three newforms are 2163188180, 4934015444, and -5895116260, respectively. In each case $a_\ell \not\equiv 0 \pmod{19}$ and $\frac{18}{\gcd\{18,15\}} = 6$, so part (3) of Theorem 2.1 again shows that $\overline{\rho}_f$ cannot be exceptional when $\ell = 19$.

For $\ell = 7, 13$, we can rule out the possibility of exceptional image as follows. Say we have a newform $f = q + \sum_{n \geq 2} a_n q^n$ in $S_{\ell-3}^{\mathrm{new}}(6)$ and a prime $p \nmid 6\ell$ such that $a_p \in \mathbb{Z}$. Setting $u(p) := a_p^2/p^9$, if the projective image of $\overline{\rho}_f$ is A_4, S_4, or A_5, then we have

$$u(p) \equiv 4, 0, 1, 2 \pmod{\ell} \quad \text{or} \quad u(p)^2 - 3u(p) + 1 \equiv 0 \pmod{\ell}, \tag{3.2}$$

depending on whether the image of $\overline{\rho}_f(\mathrm{Frob}_p)$ in $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ has order 1, 2, 3, 4, or 5 (see for example [Rib85, p. 189]). When $\ell = 7$, one can check directly that (3.2) is not satisfied when $p = 5$ for the unique newform $f \in S_4^{\mathrm{new}}(6)$ with Fourier expansion (3.1) above. When $\ell = 13$, there is again a unique newform $f \in S_{10}^{\mathrm{new}}(6)$ and it has Fourier expansion

$$f = q - 16q^2 + 81q^3 + 256q^4 + 2694q^5 + \cdots$$

by [LMF20]. We can again check directly that (3.2) is not satisfied when $p = 5$. $\square$

Remark. The conclusion of Proposition 3.3 does not hold in general for the spaces $S_{\ell^2-3}^{\mathrm{new}}(6)$; this is the main reason that we are able to say more about Type I congruences than those of Type II.

Next we will prove a few group theoretic lemmas (Lemmas 3.5, 3.6 and 3.7) leading to Proposition 3.8. Before continuing we need to introduce some notation.

Notation. Let G be a group and let $\tau \in \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$.

- For a homomorphism $\overline{\rho}\colon G \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, we write ${}^\tau\overline{\rho}\colon G \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ for the composite of $\overline{\rho}$ with the automorphism $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ induced by $\tau\colon \overline{\mathbb{F}}_\ell \to \overline{\mathbb{F}}_\ell$.
- Similarly, for a homomorphism $r\colon G \to \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$, we write ${}^\tau r\colon G \to \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ for the composite of r with the automorphism $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell) \to \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ induced by $\tau\colon \overline{\mathbb{F}}_\ell \to \overline{\mathbb{F}}_\ell$.
- For two homomorphisms $r_1, r_2\colon G \to \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$, we write $r_1 \cong r_2$ if they are conjugate by an element of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$.
- For a normalized eigenform $f \in S_k(N)$, we let $r_f\colon G_\mathbb{Q} \to \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ be the composite of $\overline{\rho}_f\colon G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ with the projection $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell) \to \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$.

Lemma 3.4. *Let $f, g \in S_k(N)$ be normalized eigenforms. If $r_f \cong r_g$ and $\overline{\rho}_f \not\cong \overline{\rho}_g$, then $\overline{\rho}_f \cong \overline{\rho}_g \otimes \omega^{\frac{\ell-1}{2}}$.*

Proof. Conjugating if necessary, we can assume that $r_f = r_g$. Then we can define a character $\eta\colon G_\mathbb{Q} \to \overline{\mathbb{F}}_\ell^\times$ by $\eta(\sigma) = \overline{\rho}_f(\sigma)\overline{\rho}_g(\sigma)^{-1}$, and we have $\overline{\rho}_f \cong \overline{\rho}_g \otimes \eta$. The lemma now follows from Lemma 3.1. $\square$

Lemma 3.5. *For $i = 1, 2$, let $\mathbb{F}_{q_i}/\mathbb{F}_\ell$ be the field of cardinality q_i in $\overline{\mathbb{F}}_\ell$, with q_i some power of ℓ, and let $r_i\colon G_\mathbb{Q} \to \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ be a continuous homomorphism with image containing $\mathrm{PSL}_2(\mathbb{F}_{q_i})$ and contained in $\mathrm{PGL}_2(\mathbb{F}_{q_i})$. Let L_i be the subfield of $\overline{\mathbb{Q}}$ fixed by $\ker(r_i)$ and let $K_i/\mathbb{Q}$ be the subextension of $L_i/\mathbb{Q}$ such that $\mathrm{Gal}(L_i/K_i) \cong \mathrm{PSL}_2(\mathbb{F}_{q_i})$. Then the following are equivalent:*

1. *$L_1 \cap L_2 \not\subseteq K_1K_2$.*
2. *$L_1 = L_2$.*
3. *There is $\tau \in \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ such that $r_1 \cong {}^\tau r_2$.*

Proof. First note that for each $i = 1, 2$, $\mathrm{PSL}_2(\mathbb{F}_{q_i})$ is simple since $|\mathbb{F}_{q_i}| \geq 4$ (recall that $\ell \geq 5$).

Clearly, (2) implies (1). On the other hand, since $\mathrm{PSL}_2(\mathbb{F}_{q_i})$ is simple and is the unique nontrivial proper normal subgroup of $\mathrm{PGL}_2(\mathbb{F}_{q_i})$, if $L_1 \cap L_2 \not\subseteq K_1K_2$, then $L_1 \subseteq L_2$ or $L_2 \subseteq L_1$, and $K_1 = K_2$. In either case, by comparing Jordan–Holder factors, we must have $L_1 = L_2$.

It is immediate that (3) implies (2). Conversely, if $L_1 = L_2$, then there is an isomorphism of groups $\varphi\colon r_1(G_\mathbb{Q}) \cong r_2(G_\mathbb{Q})$. In particular, this implies that $q_1 = q_2$. So letting $\mathbb{F}_q = \mathbb{F}_{q_1} = \mathbb{F}_{q_2}$, we have either that $r_1(G_\mathbb{Q}) = r_2(G_\mathbb{Q}) = \mathrm{PSL}_2(\mathbb{F}_q)$ and φ is an automorphism of $\mathrm{PSL}_2(\mathbb{F}_q)$, or that $r_1(G_\mathbb{Q}) = r_2(G_\mathbb{Q}) = \mathrm{PGL}_2(\mathbb{F}_q)$ and φ is an automorphism of $\mathrm{PGL}_2(\mathbb{F}_q)$. The automorphism group of both $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ is $\mathrm{PGL}_2(\mathbb{F}_q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_\ell)$ (see [Ste16, Theorem 30]), which implies that r_1 is conjugate to ${}^\tau r_2$ for some $\tau \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_\ell)$. □

Lemma 3.6. *Let $G_1, \ldots, G_s$ and H be simple nonabelian groups. Any surjective homomorphism $f\colon \prod_{i=1}^s G_i \to H$ factors through some projection $p_j\colon \prod_{i=1}^s G_i \to G_j$.*

Proof. For each $1 \leq n \leq s$, let $\iota_n\colon G_n \to \prod_{i=1}^s G_i$ be the canonical injection. Assume that f does not factor through any p_j. Then there are indices $1 \leq m \neq n \leq s$ such that $f \circ \iota_m\colon G_m \to H$ and $f \circ \iota_n\colon G_n \to H$ are nontrivial. Since G_n and G_m are simple, $f \circ \iota_m$ and $f \circ \iota_n$ are injective. Since $\iota_m(G_m)$ and $\iota_n(G_n)$ are normal subgroups of $\prod_{i=1}^s G_i$ and f is surjective, $f \circ \iota_m(G_m)$ and $f \circ \iota_n(G_n)$ are normal subgroups of H. We see that $f \circ \iota_m$ and $f \circ \iota_n$ are isomorphisms. Since H is nonabelian, we can then choose $x \in G_m$ and $y \in G_n$ such that $f \circ \iota_m(x)$ and $f \circ \iota_n(y)$ do not commute. But $\iota_m(x)$ and $\iota_n(y)$ commute in $\prod_{i=1}^s G_i$, which gives a contradiction. □

Lemma 3.7. *Let $f_1, \ldots, f_s \in S_k(N)$ be normalized eigenforms. For each $1 \leq i \leq s$, assume that $\overline{\rho}_{f_i}(G_\mathbb{Q})$ contains a conjugate of $\mathrm{SL}_2(\mathbb{F}_\ell)$, and let M_i be the subfield of $\overline{\mathbb{Q}}$ fixed by $\ker(\overline{\rho}_{f_i})$. Then we have the following.*

1. *For each $1 \leq i \leq s$, there is an extension $K_i/\mathbb{Q}$ of degree at most 2 contained in M_i and a finite extension $\mathbb{F}_{q_i}/\mathbb{F}_\ell$ such that $\overline{\rho}_{f_i}(G_{K_i(\zeta_\ell)})$ is conjugate to $\mathrm{SL}_2(\mathbb{F}_{q_i})$.*
2. *Assume moreover that for each $1 \leq i \neq j \leq s$, there is no $\tau \in \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ such that $r_{f_i} \cong {}^\tau r_{f_j}$. Let K_i and $\mathbb{F}_{q_i}$ be as in part (1), and set $M = M_1 \cdots M_s$ and $K = K_1 \cdots K_s$. Then $\mathrm{Gal}(M(\zeta_\ell)/K(\zeta_\ell)) \cong \prod_{i=1}^s \mathrm{SL}_2(\mathbb{F}_{q_i})$.*

Proof. For each $1 \leq i \leq s$, since $\overline{\rho}_{f_i}(G_\mathbb{Q})$ contains a conjugate of $\mathrm{SL}_2(\mathbb{F}_\ell)$, [DDT97, Theorem 2.47(b)] implies that the image of r_{f_i} is conjugate to either $\mathrm{PSL}_2(\mathbb{F}_{q_i})$ or $\mathrm{PGL}_2(\mathbb{F}_{q_i})$ for some finite extension $\mathbb{F}_{q_i}/\mathbb{F}_\ell$. Replacing $\overline{\rho}_{f_i}$ by a conjugate if necessary, we assume that r_{f_i} has image either $\mathrm{PSL}_2(\mathbb{F}_{q_i})$ or $\mathrm{PGL}_2(\mathbb{F}_{q_i})$. We then let $K_i/\mathbb{Q}$ be the extension of degree at most 2 such that $r_{f_i}(G_{K_i}) = \mathrm{PSL}_2(\mathbb{F}_{q_i})$, which is a simple group since $\ell \geq 5$. Then $r_{f_i}(G_{K_i}(\zeta_\ell)) = \mathrm{PSL}_2(\mathbb{F}_{q_i})$ as well, so $\overline{\rho}_{f_i}(G_{K_i(\zeta_\ell)})$ is a subgroup of $\overline{\mathbb{F}}_\ell^\times \mathrm{SL}_2(\mathbb{F}_{q_i})$ which contains $\mathrm{SL}_2(\mathbb{F}_{q_i})$ and has trivial determinant. It follows that $\overline{\rho}_{f_i}(G_{K_i(\zeta_\ell)}) = \mathrm{SL}_2(\mathbb{F}_{q_i})$.

To prove part (2), we first establish some preliminaries. For each $1 \leq i \leq s$, let L_i be the subfield of M_i fixed by $\ker(r_{f_i})$. We claim the following.

(a) $\mathrm{Gal}(L_iK(\zeta_\ell)/K(\zeta_\ell)) \cong \mathrm{PSL}_2(\mathbb{F}_{q_i})$.
(b) $\mathrm{Gal}(M_iK(\zeta_\ell)/K(\zeta_\ell)) \cong \mathrm{SL}_2(\mathbb{F}_{q_i})$.

(c) For $1 \leq i \neq j \leq s$, the fields $L_iK(\zeta_\ell)$ and $L_jK(\zeta_\ell)$ are disjoint over $K(\zeta_\ell)$.

Since $\mathrm{Gal}(L_i/K_i) \cong \mathrm{PSL}_2(\mathbb{F}_{q_i})$ is nonabelian and simple and $K(\zeta_\ell)/K_i$ is abelian, these extensions are disjoint and $\mathrm{Gal}(L_iK(\zeta_\ell)/K(\zeta_\ell)) \cong \mathrm{PSL}_2(\mathbb{F}_{q_i})$, which gives claim (a). Further, since the unique nontrivial proper quotient of

$$\mathrm{Gal}(M_iK_i(\zeta_\ell)/K_i(\zeta_\ell)) \cong \mathrm{SL}_2(\mathbb{F}_{q_i})$$

is $\mathrm{Gal}(L_iK_i(\zeta_\ell)/K_i(\zeta_\ell)) \cong \mathrm{PSL}_2(\mathbb{F}_{q_i})$, we have

$$M_iK_i(\zeta_\ell) \cap K(\zeta_\ell) \neq K_i(\zeta_\ell) \Leftrightarrow L_iK_i(\zeta_\ell) \cap K(\zeta_\ell) \neq K_i(\zeta_\ell).$$

So $M_iK_i(\zeta_\ell)$ and $K(\zeta_\ell)$ are also disjoint over $K_i(\zeta_\ell)$, which proves claim (b). We now prove claim (c). If this were not the case, we would have $L_i \subseteq L_jK(\zeta_\ell)$ or $L_j \subseteq L_iK(\zeta_\ell)$. Without loss of generality, assume that $L_i \subseteq L_jK(\zeta_\ell)$. But $\mathrm{Gal}(L_jK(\zeta_\ell)/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(L_j/\mathbb{Q}) \times \mathrm{Gal}(K(\zeta_\ell)/\mathbb{Q})$ has a unique nonabelian Jordan–Holder factor, namely the one isomorphic to $\mathrm{Gal}(L_j/K_j)$. So $L_i \subseteq L_jK(\zeta_\ell)$ implies that $\mathrm{Gal}(L_iL_j/\mathbb{Q})$ also has a unique nonabelian Jordan–Holder factor, which implies that $L_i \cap L_j \not\subseteq K_iK_j$. By Lemma 3.5, this contradicts our hypotheses on r_{f_i} and r_{f_j}.

To conclude, we prove by induction on $1 \leq j \leq s$ that

$$\mathrm{Gal}(M_1 \cdots M_jK(\zeta_\ell)/K(\zeta_\ell)) \cong \prod_{i=1}^{j} \mathrm{Gal}(M_iK(\zeta_\ell)/K(\zeta_\ell)) \cong \prod_{i=1}^{j} \mathrm{SL}_2(\mathbb{F}_{q_i}).$$

The $j = 1$ case follows from claim (b) of the previous paragraph. Now take $1 \leq j-1 \leq s$, and assume that

$$\mathrm{Gal}(M_1 \cdots M_{j-1}K(\zeta_\ell)/K(\zeta_\ell)) \cong \prod_{i=1}^{j-1} \mathrm{Gal}(M_iK(\zeta_\ell)/K(\zeta_\ell)) \cong \prod_{i=1}^{j-1} \mathrm{SL}_2(\mathbb{F}_{q_i}).$$

We want to show that $M_1 \cdots M_{j-1}K(\zeta_\ell)$ and $M_jK(\zeta_\ell)$ are disjoint over $K(\zeta_\ell)$. Assume otherwise. Since $\mathrm{Gal}(L_jK(\zeta_\ell)) \cong \mathrm{PSL}_2(\mathbb{F}_{q_j})$ is the unique nontrivial proper quotient of $\mathrm{Gal}(M_jK(\zeta_\ell)/K(\zeta_\ell)) \cong \mathrm{SL}_2(\mathbb{F}_{q_j})$, we must then have $L_jK(\zeta_\ell) \subseteq M_1 \cdots M_{j-1}K(\zeta_\ell)$. Since $\mathrm{Gal}(L_jK(\zeta_\ell)/K(\zeta_\ell))$ is nonabelian simple, the centre of $\prod_{i=1}^{j-1} \mathrm{SL}_2(\mathbb{F}_{q_i})$ maps trivially under the surjective morphism

$$\prod_{i=1}^{j-1} \mathrm{SL}_2(\mathbb{F}_{q_i}) \cong \mathrm{Gal}(M_1 \cdots M_{j-1}K(\zeta_\ell)/K(\zeta_\ell)) \to \mathrm{Gal}(L_jK(\zeta_\ell)/K(\zeta_\ell)),$$

and this map factors through

$$\prod_{i=1}^{j-1} \mathrm{PSL}_2(\mathbb{F}_{q_i}) \cong \prod_{i=1}^{j-1} \mathrm{Gal}(L_iK(\zeta_\ell)/K(\zeta_\ell)).$$

By Lemma 3.6, this map further factors through some $\mathrm{Gal}(L_iK(\zeta_\ell)/K(\zeta_\ell))$ with $1 \leq i \leq j-1$. But this implies that $L_jK(\zeta_\ell) \subseteq L_iK(\zeta_\ell)$, contradicting claim (c) from the previous paragraph. This concludes the proof. □

Proposition 3.8. *Let $f_1, \ldots, f_s \in S_k(N)$ be normalized eigenforms such that for each $1 \leq i \leq s$, $\overline{\rho}_{f_i}(G_\mathbb{Q})$ contains a conjugate of $\mathrm{SL}_2(\mathbb{F}_\ell)$. Then for any $\gamma \in \mathrm{SL}_2(\mathbb{F}_\ell)$, there is an element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell))$ such that $\overline{\rho}_{f_i}(\sigma)$ is conjugate to γ for each $1 \leq i \leq s$.*

Proof. Say $r_{f_i} \cong {}^\tau r_{f_j}$ for some $i \neq j$ and $\tau \in \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$. Then by Lemma 3.4, $\overline{\rho}_{f_i}(\sigma)$ is conjugate to ${}^\tau\overline{\rho}_{f_j}(\sigma)$ for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell))$. If further $\overline{\rho}_{f_j}(\sigma)$ is conjugate to $\gamma \in \mathrm{SL}_2(\mathbb{F}_\ell)$, then ${}^\tau\overline{\rho}_{f_j}(\sigma)$ is conjugate to γ as well. We can thus assume that for each $1 \leq i \neq j \leq s$, there is no $\tau \in \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ such that $r_{f_i} \cong {}^\tau r_{f_j}$. The result now follows from Lemma 3.7. □

We can now prove Theorem 1.5, using Propositions 3.3 and 3.8 as a base case for induction.

Proof of Theorem 1.5. Choose a number field E containing all Fourier coefficients of all the newforms in $S_{\ell-3}^{\mathrm{new}}(6)$. Let λ be the prime of E induced by our fixed embedding $\iota_\ell \colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. Let E_λ be the completion of E at λ, let $\mathcal{O}_\lambda$ be its ring of integers, and let $\mathbb{F} = \mathcal{O}_\lambda/\lambda$ be the residue field. Then for any newform $f \in S_{\ell-3}^{\mathrm{new}}(6)$, the Galois representations ρ_f and $\overline{\rho}_f$ of Theorem 2.1 can be defined over $\mathcal{O}_\lambda$ and $\mathbb{F}$, respectively. By Lemma 2.3, there is an integer $r \geq m$ such that it suffices to show that there is a positive density set of primes Q with $Q \equiv 1 \pmod{\ell^m}$ and $f\big|T(Q) \equiv f \pmod{\lambda^r}$ for all newforms $f \in S_{\ell-3}^{\mathrm{new}}(6)$.

By Propositions 3.3 and 3.8, we can find an element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell))$ such that $\overline{\rho}_f(\sigma)$ is conjugate to $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ for any newform $f \in S_{\ell-3}^{\mathrm{new}}(6)$. In particular, $\rho_f(\sigma)$ has characteristic polynomial congruent to $x^2 - x + 1 \pmod{\lambda}$. Enlarging E if necessary, we can assume that $x^2 - x + 1$ factors in $\mathbb{F}$ and its roots are the two primitive 6-th roots of unity, which we denote by ξ and ξ'. Since ξ and ξ' are distinct, we can factor the characteristic polynomial of $\rho_f(\sigma)$ over $\mathcal{O}_\lambda$ by Hensel's lemma, and $\rho_f(\sigma)$ is conjugate to a diagonal matrix with entries α, β such that $\alpha \equiv \xi \pmod{\lambda}$ and $\beta \equiv \xi' \pmod{\lambda}$. Letting ξ and ξ' again denote the primitive 6-th roots of unity in $\mathcal{O}_\lambda$, we write $\alpha = \xi\gamma$ and $\beta = \xi'\delta$ with $\gamma, \delta \equiv 1 \pmod{\lambda}$. Now $\rho_f(\sigma^{\ell^{r-1}})$ is conjugate to a diagonal matrix with entries $\alpha^{\ell^{r-1}} = \xi^{\ell^{r-1}}\gamma^{\ell^{r-1}}$ and $\beta^{\ell^{r-1}} = \xi'^{\ell^{r-1}}\delta^{\ell^{r-1}}$. Observe that both $\gamma^{\ell^{r-1}}$ and $\delta^{\ell^{r-1}}$ are congruent to 1 modulo λ^r (recall that $\lambda|\ell$), and that $\{\xi^{\ell^{r-1}}, \xi'^{\ell^{r-1}}\} = \{\xi, \xi'\}$. Thus the characteristic polynomial of $\rho_f(\sigma^{\ell^{r-1}})$ is congruent to $(x-\xi)(x-\xi') = x^2 - x + 1$ modulo λ^r. Also, $\sigma^{\ell^{r-1}} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_{\ell^m}))$ since $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^m})/\mathbb{Q}(\zeta_\ell))$ has order ℓ^{m-1} and $r \geq m$. Chebotarev's density theorem implies that for a positive density set of primes Q, Frob_Q is conjugate to $\sigma^{\ell^{r-1}}$. For such Q, we have $Q \equiv 1 \pmod{\ell^m}$ and for any newform $f \in S_{\ell-3}^{\mathrm{new}}(6)$, we have

$$f\big|T(Q) = (\operatorname{tr}\rho_f(\mathrm{Frob}_Q))f \equiv f \pmod{\lambda^r}.$$

The theorem is now proven. □

4. Congruences in arbitrary weight

In this section, we use a different argument to prove two variants of Theorem 1.5 in arbitrary integral weight $k \geq 2$ with additional hypotheses on the prime ℓ. It will be convenient for us to fix a number field E containing all Fourier coefficients of all newforms in $S_k^{\mathrm{new}}(6, \varepsilon_2, \varepsilon_3)$. Let λ be the prime of E induced by our fixed embedding $\iota_\ell \colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ and let e be the ramification index.

We begin with an elementary lemma.

Lemma 4.1. *If a is an integer with $2^a \equiv -2 \pmod{\ell}$, then $2^{\ell^{m-1}(a-1)+1} \equiv -2 \pmod{\ell^m}$ for any $m \geq 1$.*

Proof. We induct on m. Suppose that $2^b \equiv -1 \pmod{\ell^m}$, and write

$$2^{\ell b} + 1 = (2^b + 1)\left((2^b)^{\ell-1} - (2^b)^{\ell-2} + \cdots - 2^b + 1\right).$$

Each summand in the second factor is 1 modulo ℓ, and there are ℓ summands, so the second term is divisible by ℓ. □

Theorem 4.2. *Suppose that $\ell \geq 5$ is prime and that there exists an integer a for which $2^a \equiv -2 \pmod{\ell}$. Let m be a natural number and let $\varepsilon_2, \varepsilon_3 \in \{\pm 1\}$. Then a positive proportion of primes $Q \equiv -2 \pmod{\ell^m}$ have the following property: for every $f \in S_k^{\mathrm{new}}(6, \varepsilon_2, \varepsilon_3)$, we have $f\big|T(Q) \equiv -(-\varepsilon_2)^a Q^{\frac{k-2}{2}} f \pmod{\ell^m}$.*

Proof. Let E_λ be the completion of E at λ, let $\mathcal{O}_\lambda$ be its ring of integers, and let $\mathbb{F} = \mathcal{O}_\lambda/\lambda$ be the residue field. Then for any newform $f \in S_k^{\mathrm{new}}(6, \varepsilon_2, \varepsilon_3)$, the Galois representations ρ_f and $\overline{\rho}_f$ of Theorem 2.1 can be defined over $\mathcal{O}_\lambda$ and $\mathbb{F}$, respectively. By Lemma 2.3 and the remark that follows it, there is an integer $r \geq m$ such that it suffices to show there is a positive proportion of primes $Q \equiv -2 \pmod{\ell^m}$ with the property that for every newform $f \in S_k^{\mathrm{new}}(6, \varepsilon_2, \varepsilon_3)$, we have $f\big|T(Q) \equiv -(-\varepsilon_2)^a Q^{\frac{k-2}{2}} f \pmod{\lambda^r}$. By Lemma 4.1, $2^{\ell^{r-1}(a-1)+1} \equiv -2 \pmod{\ell^r}$. Since a and $\ell^{r-1}(a-1)+1$ have the same parity, we can replace a with $\ell^{r-1}(a-1)+1$ and assume that $2^a \equiv -2 \pmod{\ell^r}$.

We have $(\rho_f|_{G_2})^{\mathrm{ss}} \cong \chi\psi \oplus \psi$ for the unramified character $\psi\colon G_2 \to \mathcal{O}_\lambda^\times$ with $\psi(\mathrm{Frob}_2) = \iota_\ell(a_2)$. By [AL70, Theorem 3], $a_2 = -\varepsilon_2 2^{\frac{k-2}{2}}$. Let K be the fixed field of the kernel of $\rho_f \bmod \lambda^r$. By Chebotarev's density theorem, a positive proportion of primes Q have Frob_Q conjugate to Frob_2^a in $\mathrm{Gal}(K(\zeta_{\ell^r})/\mathbb{Q})$. For such Q, we have

$$Q \equiv \chi(\mathrm{Frob}_Q) \equiv \chi(\mathrm{Frob}_2^a) \equiv 2^a \equiv -2 \pmod{\ell^r}.$$

We also have

$$\begin{aligned} a_Q = \operatorname{tr}\rho_f(\mathrm{Frob}_Q) \equiv \operatorname{tr}\rho_f(\mathrm{Frob}_2^a) &\equiv (-\varepsilon_2 2^{\frac{k-2}{2}})^a 2^a + (-\varepsilon_2 2^{\frac{k-2}{2}})^a \\ &\equiv (-\varepsilon_2)^a 2^{a\frac{k-2}{2}}(2^a+1) \equiv -(-\varepsilon_2)^a Q^{\frac{k-2}{2}} \mod \lambda^r. \end{aligned}$$

The theorem is now proven. □

A similar argument establishes Theorem 4.3, albeit with a stronger hypothesis and slightly weaker conclusion (due to the lack of an analogue of Lemma 4.1).

Theorem 4.3. *Suppose that $\ell \geq 5$ is prime, that m is a natural number, and that there exists an integer a such that $3^a \equiv -2 \pmod{\ell^m}$. Then a positive proportion of primes $Q \equiv -2 \pmod{\ell^m}$ have the following property: for every newform $f \in S_k^{\mathrm{new}}(6, \varepsilon_2, \varepsilon_3)$, we have $f\big|T(Q) \equiv -(-\varepsilon_3)^a Q^{\frac{k-2}{2}} f \pmod{\lambda^{em}}$.*

Proof. We proceed as in Theorem 4.2 with 2 replaced by 3 and $r = em$. □

5. The application to partitions

We use the results of the last two sections to prove Theorems 1.2 – 1.4 from Section 1. We begin with Lemmas 5.1 and 5.2.

Lemma 5.1. *Let $\ell \geq 5$ be prime, and suppose that $f \in S_k\left(1, \nu_\eta^r, \mathbb{Z}\right)$ where $(r, 24) = 1$ and $k \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$. Suppose that $Q \geq 5$ is a prime and that λ_Q is an integer with*

$$g\big|T(Q) \equiv \lambda_Q g \pmod{\ell} \quad \text{for all} \;\; g \in S_{2k-1}^{\text{new}}\left(6, -\left(\frac{8}{r}\right), -\left(\frac{12}{r}\right), \mathbb{Z}\right).$$

Then

$$f\big|T(Q^2) \equiv \left(\frac{12}{Q}\right) \lambda_Q f \pmod{\ell}.$$

Proof. For each squarefree t let

$$F_t \in S_{2k-1}^{\text{new}}\left(6, -\left(\frac{8}{r}\right), -\left(\frac{12}{r}\right), \mathbb{Z}\right)$$

be the form with

$$\operatorname{Sh}_t f = F_t \otimes \left(\frac{12}{\bullet}\right).$$

For each t we have

$$\left(F_t \otimes \left(\frac{12}{\bullet}\right)\right) \big|T(Q) = \left(\frac{12}{Q}\right) \left(F_t\big|T(Q)\right) \otimes \left(\frac{12}{\bullet}\right) \equiv \left(\frac{12}{Q}\right) \lambda_Q F_t \otimes \left(\frac{12}{\bullet}\right) \pmod{\ell}.$$

In other words, for each squarefree t we have

$$\operatorname{Sh}_t(f\big|T(Q^2)) = (\operatorname{Sh}_t f)\big|T(Q) \equiv \left(\frac{12}{Q}\right) \lambda_Q \operatorname{Sh}_t f \pmod{\ell}.$$

The lemma now follows from (2.5). ☐

Lemma 5.2 describes the consequence of finding a "good" eigenvalue.

Lemma 5.2. *Let $\ell \geq 5$ be prime, and suppose that $f \in S_k\left(1, \nu_\eta^r, \mathbb{Z}\right)$ where $(r, 24) = 1$ and $k \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$. Suppose that $Q \geq 5$ is prime and that there exists $\alpha_Q \in \{\pm 1\}$ with*

$$f\big|T(Q^2) \equiv \alpha_Q Q^{k-\frac{3}{2}} f \pmod{\ell}.$$

Then we have

$$a(Q^2 n) \equiv 0 \pmod{\ell} \quad \text{if} \quad \left(\frac{n}{Q}\right) = \alpha_Q \left(\frac{12}{Q}\right) \left(\frac{-1}{Q}\right)^{k-\frac{1}{2}}.$$

Proof. This follows from (2.4). For such n, the middle term in the definition of the Hecke operator cancels against the same term in $\alpha_Q Q^{k-\frac{3}{2}} f$, and the third term does not contribute. ☐

Proof of Theorem 1.2. For $\ell \geq 13$, let $f_\ell = \sum a(n) q^{\frac{n}{24}} \in S_{\frac{\ell-2}{2}}\left(1, \nu_\eta^{-\ell}, \mathbb{Z}\right)$ be the modular form in (2.6). By Theorem 1.5, a positive proportion of primes $Q \equiv 1 \pmod{\ell}$ have the property that for all $g \in S_{\ell-3}^{\text{new}}\left(6, -\left(\frac{8}{-\ell}\right), -\left(\frac{12}{-\ell}\right)\right)$ we have

$$g\big|T(Q) \equiv g \pmod{\ell}.$$

For such primes it follows from Lemma 5.1 that

$$f_\ell\big|T(Q^2) \equiv \left(\frac{12}{Q}\right) f_\ell \pmod{\ell}.$$

Since $a(n) \equiv p\left(\frac{\ell n+1}{24}\right) \pmod{\ell}$, it follows from Lemma 5.2 that

$$p\left(\frac{Q^2\ell n+1}{24}\right) \equiv 0 \pmod{\ell} \qquad \text{if} \qquad \left(\frac{n}{Q}\right) = \left(\frac{-1}{Q}\right)^{\frac{\ell-3}{2}}.$$

$\square$

Proof of Theorem 1.3. Suppose that $\ell \geq 13$ is a prime such that $2^a \equiv -2 \pmod{\ell}$ for some a. Theorem 4.2 guarantees that there exist $\beta \in \{\pm 1\}$ and a positive proportion of primes $Q \equiv -2 \pmod{\ell}$ such that

(5.1)

$$g\big|T(Q) \equiv \beta Q^{\frac{\ell-5}{2}} g \pmod{\ell} \quad \text{for all} \quad g \in S^{\text{new}}_{\ell-3}\left(6, -\left(\frac{8}{-\ell}\right), -\left(\frac{12}{-\ell}\right), \mathbb{Z}\right).$$

It follows from Lemma 5.1 that

$$f_\ell\big|T(Q^2) \equiv \left(\frac{12}{Q}\right) \beta Q^{\frac{\ell-5}{2}} f_\ell \pmod{\ell}.$$

From Lemma 5.2 we conclude that there are Type I congruences for such primes Q.

To prove the existence of Type II congruences for $\ell \geq 5$ we argue in a similar way, starting with the modular form $g_\ell = \sum b(n) q^{\frac{n}{24}} \in S_{\frac{\ell^2-2}{2}}\left(1, \nu_\eta^{-1}, \mathbb{Z}\right)$ defined in (2.7). In this case we have

$$b(n) \equiv p\left(\frac{n+1}{24}\right) \pmod{\ell} \quad \text{when} \quad \left(\frac{-n}{\ell}\right) = -1.$$

By (2.8) we have $\varepsilon_2 = -1$ in Theorem 4.2; we conclude using that result and Lemma 5.1 that for a positive proportion of primes $Q \equiv -2 \pmod{\ell}$ we have

$$g_\ell\big|T(Q^2) \equiv -\left(\frac{12}{Q}\right) Q^{\frac{\ell^2-5}{2}} g_\ell \pmod{\ell}.$$

By Lemma 5.2 we conclude that

$$b(Q^2 n) \equiv 0 \pmod{\ell} \quad \text{if} \quad \left(\frac{n}{Q}\right) = -\left(\frac{-1}{Q}\right)^{\frac{\ell^2-3}{2}} = -\left(\frac{-1}{Q}\right),$$

which gives a congruence of the form (1.7). $\square$

Finally, we turn to the proof of Theorem 1.4. Here the situation is complicated by the lack of an analogue of Lemma 4.1 for the prime 3; this necessitates the added assumption that there are no congruences between newforms in the relevant spaces. We first need a straightforward lemma.

Lemma 5.3. *Suppose that the space* $S^{\text{new}}_k(6, \varepsilon_2, \varepsilon_3)$ *(where k is even) is spanned by newforms* $g_1, \ldots, g_d$. *Let E be a number field containing the coefficients of* $g_1, \ldots g_d$, *let $\mathcal{O}$ be the ring of integers and let λ be a prime of E over the rational prime ℓ. Suppose that there is no congruence* $g_i \equiv g_j \pmod{\lambda}$ *with* $i \neq j$. *Then if a nonzero modular form* $F \in S^{\text{new}}_k(6, \varepsilon_2, \varepsilon_3, \mathcal{O})$ *is expressed as a linear combination*

$$F = \sum_{i=1}^{d} c_i g_i \qquad \textit{with } c_i \in E, \tag{5.2}$$

we have $\operatorname{ord}_\lambda(c_i) \geq 0$ *for all* i.

Proof. If the conclusion were false, then clearing denominators in (5.2) would show that the set $\{g_1, \ldots, g_d\}$ is linearly dependent over $\mathcal{O}/\lambda$. Let $j < d$ be the maximal index for which $\{g_1, \ldots, g_j\}$ is linearly independent over $\mathcal{O}/\lambda$. Then there is a relation

$$g_{j+1} \equiv \sum_{i=1}^{j} \alpha_i g_i \pmod{\lambda}. \tag{5.3}$$

Write $g_i = \sum b_i(n)q^n$, and assume without loss of generality that $\alpha_1 \not\equiv 0 \pmod{\lambda}$. By assumption we can find a prime $p \geq 5$ for which

$$b_{j+1}(p) \not\equiv b_1(p) \pmod{\lambda}.$$

Applying the Hecke operator $T(p)$ to (5.3) gives

$$b_{j+1}(p) \sum_{i=1}^{j} \alpha_i g_i \equiv \sum_{i=1}^{j} b_i(p)\alpha_i g_i.$$

Since $\alpha_1(b_{j+1}(p) - b_1(p)) \not\equiv 0 \pmod{\lambda}$, this gives a contradiction. □

Proof of Theorem 1.4. Suppose that $\ell \geq 13$ is a prime such that $3^a \equiv -2 \pmod{\ell}$ for some a. Applying Theorem 4.3 with $m = 1$ shows that there exist $\beta \in \{\pm 1\}$ and a positive proportion of primes $Q \equiv -2 \pmod{\ell}$ such that for every newform $g \in S^{\mathrm{new}}_{\ell-3}\left(6, -\left(\frac{8}{-\ell}\right), -\left(\frac{12}{-\ell}\right)\right)$ we have

$$g\big|T(Q) \equiv \beta Q^{\frac{\ell-5}{2}} g \pmod{\lambda}.$$

By Lemma 5.3 it follows that (5.1) holds, and we argue as before to obtain the first conclusion of Theorem 1.4. The second conclusion follows in similar fashion. □

Acknowledgments

We thank Frank Calegari, Robert Dicks, J.-P. Serre, and the anonymous referee for helpful comments on a previous version of this manuscript.

References

[AB03] Scott Ahlgren and Matthew Boylan, *Arithmetic properties of the partition function*, Invent. Math. **153** (2003), no. 3, 487–502, DOI 10.1007/s00222-003-0295-6. MR2000466

[ABR] Scott Ahlgren, Olivia Beckwith, and Martin Raum, *Scarcity of congruences for the partition function*, Amer. J. Math., 2022 (to appear).

[ACC+] Patrick B. Allen, Frank Calegari, Ana Caraiani, Toby Gee, David Helm, Bao V. Le Hung, James Newton, Peter Scholze, Richard Taylor, and Jack A. Thorne, *Potential automorphy over CM fields*, Ann. of Math., 2022 To appear.

[Ahl00] Scott Ahlgren, *Distribution of the partition function modulo composite integers M*, Math. Ann. **318** (2000), no. 4, 795–803, DOI 10.1007/s002080000142. MR1802511

[AL70] A. O. L. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(m)$*, Math. Ann. **185** (1970), 134–160, DOI 10.1007/BF01359701. MR268123

[AO67] A. O. L. Atkin and J. N. O'Brien, *Some properties of $p(n)$ and $c(n)$ modulo powers of* 13, Trans. Amer. Math. Soc. **126** (1967), 442–459, DOI 10.2307/1994308. MR214540

[AO01a] Scott Ahlgren and Ken Ono, *Congruence properties for the partition function*, Proc. Natl. Acad. Sci. USA **98** (2001), no. 23, 12882–12884, DOI 10.1073/pnas.191488598. MR1862931

[AO01b] Scott Ahlgren and Ken Ono, *Congruences and conjectures for the partition function*, q-series with applications to combinatorics, number theory, and physics (Urbana, IL, 2000), Contemp. Math., vol. 291, Amer. Math. Soc., Providence, RI, 2001, pp. 1–10, DOI 10.1090/conm/291/04889. MR1874518

[Atk67] A. O. L. Atkin, *Proof of a conjecture of Ramanujan*, Glasgow Math. J. **8** (1967), 14–32, DOI 10.1017/S0017089500000045. MR205958

[Atk68] A. O. L. Atkin, *Multiplicative congruence properties and density problems for $p(n)$*, Proc. London Math. Soc. (3) **18** (1968), 563–576, DOI 10.1112/plms/s3-18.3.563. MR227105

[Car89] Henri Carayol, *Sur les représentations galoisiennes modulo l attachées aux formes modulaires* (French), Duke Math. J. **59** (1989), no. 3, 785–801, DOI 10.1215/S0012-7094-89-05937-1. MR1046750

[DDT97] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), Int. Press, Cambridge, MA, 1997, pp. 2–140. MR1605752

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR2112196

[Edi92] Bas Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594, DOI 10.1007/BF01232041. MR1176206

[Has66] Helmut Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung* mod.p *ist* (German), Math. Ann. **166** (1966), 19–23, DOI 10.1007/BF01361432. MR205975

[Hid00] Haruzo Hida, *Modular forms and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 69, Cambridge University Press, Cambridge, 2000, DOI 10.1017/CBO9780511526046. MR1779182

[Joh12] Fredrik Johansson, *Efficient implementation of the Hardy-Ramanujan-Rademacher formula*, LMS J. Comput. Math. **15** (2012), 341–359, DOI 10.1112/S1461157012001088. MR2988821

[Kno70] Marvin I. Knopp, *Modular functions in analytic number theory*, Markham Publishing Co., Chicago, Ill., 1970. MR0265287

[LMF20] The LMFDB Collaboration, *The L-functions and modular forms database*, 2020, `http://www.lmfdb.org`.

[New57] Morris Newman, *Congruences for the coefficients of modular forms and some new congruences for the partition function*, Canadian J. Math. **9** (1957), 549–552, DOI 10.4153/CJM-1957-062-1. MR92801

[Ono00] Ken Ono, *Distribution of the partition function modulo m*, Ann. of Math. (2) **151** (2000), no. 1, 293–307, DOI 10.2307/121118. MR1745012

[Rad13] Cristian-Silviu Radu, *Proof of a conjecture by Ahlgren and Ono on the non-existence of certain partition congruences*, Trans. Amer. Math. Soc. **365** (2013), no. 9, 4881–4894, DOI 10.1090/S0002-9947-2013-05777-7. MR3066773

[Ram19] S. Ramanujan, *Some properties of $p(n)$, the number of partitions of n*, Proc. Cambridge Philos. Soc. **19** (1919), 207–210. MR2280868

[Ram20] S. Ramanujan, *Congruence properties of partitions*, Proc. London Math. Soc (Records for 13 March 1919) (1920). MR2280871

[Ram21] S. Ramanujan, *Congruence properties of partitions*, Math. Z. **9** (1921), no. 1-2, 147–153, DOI 10.1007/BF01378341. MR1544457

[Rau21] Martin Raum, *Relations among Ramanujan-type congruences II*, `arXiv:2105.13170`, 2021.

[Rib85] Kenneth A. Ribet, *On l-adic representations attached to modular forms. II*, Glasgow Math. J. **27** (1985), 185–194, DOI 10.1017/S0017089500006170. MR819838

[Ser76] Jean-Pierre Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseign. Math. (2) **22** (1976), no. 3-4, 227–260. MR434996

[Ser87] Jean-Pierre Serre, *Sur les représentations modulaires de degré* 2 *de* Gal$(\overline{\mathbf{Q}}/\mathbf{Q})$ (French), Duke Math. J. **54** (1987), no. 1, 179–230, DOI 10.1215/S0012-7094-87-05413-5. MR885783

[Ser12] Jean-Pierre Serre, *Lectures on $N_X(p)$*, Chapman & Hall/CRC Research Notes in Mathematics, vol. 11, CRC Press, Boca Raton, FL, 2012. MR2920749

[Shi73] Goro Shimura, *On modular forms of half integral weight*, Ann. of Math. (2) **97** (1973), 440–481, DOI 10.2307/1970831. MR332663

[Ste16] Robert Steinberg, *Lectures on Chevalley groups*, University Lecture Series, vol. 66, American Mathematical Society, Providence, RI, 2016. Notes prepared by John Faulkner and Robert Wilson; Revised and corrected edition of the 1968 original [MR0466335]; With a foreword by Robert R. Snapp, DOI 10.1090/ulect/066. MR3616493

[Tre06] Stephanie Treneer, *Congruences for the coefficients of weakly holomorphic modular forms*, Proc. London Math. Soc. (3) **93** (2006), no. 2, 304–324, DOI 10.1112/S0024611506015814. MR2251155

[Tre08] Stephanie Treneer, *Quadratic twists and the coefficients of weakly holomorphic modular forms*, J. Ramanujan Math. Soc. **23** (2008), no. 3, 283–309. MR2446602

[Wat38] G. N. Watson, *Ramanujans Vermutung über Zerfällungszahlen* (German), J. Reine Angew. Math. **179** (1938), 97–128, DOI 10.1515/crll.1938.179.97. MR1581588

[Wea01] Rhiannon L. Weaver, *New congruences for the partition function*, Ramanujan J. **5** (2001), no. 1, 53–63, DOI 10.1023/A:1011493128408. MR1829808

[Yan14] Yifan Yang, *Modular forms of half-integral weights on* $\mathrm{SL}(2,\mathbb{Z})$, Nagoya Math. J. **215** (2014), 1–66, DOI 10.1215/00277630-2684452. MR3263525

Department of Mathematics, University of Illinois, Urbana, Illinois 61801
Email address: `sahlgren@illinois.edu`

Department of Mathematics and Statistics, McGill University, Montreal, Quebec H3A 0B9, Canada
Email address: `patrick.allen@mcgill.ca`

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907
Email address: `tang573@purdue.edu`