manuscripta math. 167, 405–434 (2022)
© The Author(s), under exclusive licence to Springer-Verlag GmbH, DE part of Springer Nature 2021

Siegfried Böcherer · Soumya Das

On Fourier coefficients of elliptic modular forms mod ℓ with applications to Siegel modular forms

Received: 31 January 2020 / Accepted: 13 January 2021 /
Published online: 13 February 2021

Abstract. We study several aspects of nonvanishing Fourier coefficients of elliptic modular forms mod ℓ, partially answering a question of Bellaïche-Soundararajan concerning the asymptotic formula for the count of the number of Fourier coefficients upto x which do not vanish mod ℓ. We also propose a precise conjecture as a possible answer to this question. Further, we prove several results related to the nonvanishing of arithmetically interesting (e.g., primitive or fundamental) Fourier coefficients mod ℓ of a Siegel modular form with integral algebraic Fourier coefficients provided ℓ is large enough. We also make some efforts to make this "largeness" of ℓ effective.

1. Introduction

The aim of this article is to obtain mod ℓ versions of some of the nonvanishing results on the Fourier coefficients of Siegel modular forms. On the one hand, over **C** such results (cf. [1,7,21]) have played important roles in many questions on automorphic forms, and it seems interesting to investigate to what extent they hold over other rings, possibly in a quantitative fashion. As an example, in [7] it was proved that for any holomorphic Siegel modular form F of degree n, there exist infinitely many inequivalent (modulo the unimodular group) half-integral matrices T whose discriminants are fundamental, such that $a_F(T) \neq 0$. Such results have several applications to automorphic representations.

On the other hand, the theory of modular forms mod ℓ has undergone extensive development since the works of Serre, Swinnerton-Dyer. Let f be an elliptic cuspidal newform of weight k, level $\Gamma_0(N)$ and $\mathfrak{l}$ is a prime ideal in the ring of integers $\mathcal{O}_K$ of a field K which lies over the odd prime ℓ. Let us define

$$\pi(f, x; \mathfrak{l}) := \{n \leq x | \, a(f, n) \not\equiv 0 \bmod \mathfrak{l}\}.$$

Serre used the Chebotarev density theorem applied to the setting of the Galois representation attached to f, and in addition the Selberg-Delange method, to deduce that for such $\mathfrak{l} \mid \ell$ and f not constant mod $\mathfrak{l}$,

S. Böcherer: Institut für Mathematik, Universität Mannheim, 68131 Mannheim, Germany.
e-mail: boecherer@math.uni-mannheim.de

S. Das: Department of Mathematics, Indian Institute of Science, Bangalore 560012, India

S. Das (✉): Humboldt Fellow, Universität Mannheim, Mannheim, Germany.
e-mail: soumya@iisc.ac.in; sdas@mail.uni-mannheim.de

Mathematics Subject Classification: Primary 11F30 · 11F46 · Secondary 11F50

https://doi.org/10.1007/s00229-021-01277-8

$$\#\pi(f,x;\mathfrak{l}) \sim c(f;\mathfrak{l})\frac{x}{(\log x)^{\alpha(f;\mathfrak{l})}} \tag{1.1}$$

for some $c(f;\mathfrak{l}), \alpha(f;\mathfrak{l}) > 0$. More recently, by the works of Bellaiche, Soundararajan, Green [4–6], quantitative results like (1.1) has been extended to arbitrary modular forms, possibly with half-integral weights.

In the first half of the paper (Sect. 3), we show that a simple sieving of newforms (inspired by [4] and relying essentially on strong multiplicity-one for $M_k(\Gamma_1(N))$) leads to quantitative results similar to (1.1) for *arbitrary* modular forms in $M_k(\Gamma_1(N))$ of the *correct* order of magnitude, when ℓ is large enough. Actually our results hold for all ℓ not dividing a fixed algebraic integer in a number field, see below, and Sect. 3.1 for more details. This technique of sieving newforms has been useful in many places e.g. [1,10] and can also be adapted to count square-free integers n for which $a(f,n) \not\equiv 0 \bmod \mathfrak{l}$, see Proposition 3.10. In general this method works whenever a space of modular forms has the strong multiplicity-one property, and the corresponding eigenforms (or newforms) possess the suitable properties in question.

Let us explain the results of this article in some detail. In Sect. 3, we prove several results about the Fourier coefficients mod $\mathfrak{l}$ of modular forms in $M_k(\Gamma_1(N))$, the mainstay being Proposition 3.4. In particular in Theorem 3.7, we show an analogue of 'oldform' theory for modular forms mod $\mathfrak{l}$ with fixed weight and level for all $\mathfrak{l}$ not dividing a certain algebraic integer $\mathcal{L}$. This has an application to a result on Siegel modular forms about non-zero 'primitive' Fourier coefficients mod $\mathfrak{l}$, see Theorem 4.4. Our method however certainly does not generally work on the bigger space of modular forms mod ℓ of level N (let us denote it by $\widetilde{M}(N)$) as eg. in [5], because after all by Jochnowitz [14] the number of systems of eigenvalues mod ℓ for any $(\ell, 6N) = 1$ is finite. But for those $f \in \widetilde{M}(N)$ which are finite linear combinations of eigenforms with pairwise distinct system of eigenvalues mod $\mathfrak{l}$, the method clearly still works.

We next note several applications of Proposition 3.4. To discuss some of these, let us introduce some notation. Let $f \in M_k(\Gamma_1(N))$ be such that its Fourier coefficients belong to the ring of integers $\mathcal{O}_K$ of a number field K. Consider a basis $\{f_1, f_2, \ldots, f_s\}$ of newforms of weight k and level dividing N, including Eisenstein-newforms (cf. [26]). Let their Fourier expansions be written as

$$f_i(\tau) = \sum_{n=0}^{\infty} b_i(n)q^n, \tag{1.2}$$

normalised so that $b_i(1) = 1$ for all i. For each pair $i \neq j$, let $m_{i,j}$ be the smallest prime coprime to N such that $b_i(m_{i,j}) \neq b_j(m_{i,j})$. For the rest of the paper, we put

$$\mathcal{L} := \prod_{i \neq j} \left(b_i(m_{i,j}) - b_j(m_{i,j})\right). \tag{1.3}$$

(Note that $\mathcal{L}$ depends on $m_{i,j}$, N, k. Later we would use some variants of $\mathcal{L}$ however, cf. Sect. 3.1.) Let $\mathfrak{l} \in \mathcal{O}_K$ be any prime lying over $\ell \in \mathbf{Z}$ such that $\mathfrak{l} \nmid \mathcal{L}$. Note that the primes $m_{i,j}$ do not depend on f. In course of this paper, we will call such a set of primes (perhaps with additional conditions, see Sect. 3.1) to be 'admissible' for the modular form at hand.

In one of our results (cf. Proposition 3.10) we show that the quantity $\pi(f, x; \mathfrak{l})$ satisfies

$$\#\pi(f, x; \mathfrak{l}) := \{n \leq x | a(f, n) \not\equiv 0 \bmod \mathfrak{l}\} \asymp \frac{x}{(\log x)^{\alpha(f;\mathfrak{l})}} \qquad (\ell \text{ odd}), \quad (1.4)$$

for some $3/4 \geq \alpha(f; \mathfrak{l}) > 0$ whenever f is non-constant mod $\mathfrak{l}$, $k \geq 1$ and $\mathfrak{l} \nmid \mathcal{L}$. These should be compared to the results in [5], which are actually valid for the algebra $\widetilde{M}(N)$ consisting of all modular forms mod $\mathfrak{l}$ on $\Gamma_1(N)$ with Fourier coefficients in O_K and is an asymptotic formula. One of our results (cf. (1.4)) in fact show that in their asymptotic formula in [5], namely

$$\#\pi(f, x, \mathfrak{l}) \sim \frac{x(\log\log x)^{h(f;\mathfrak{l})}}{(\log x)^{\alpha(f;\mathfrak{l})}} \qquad (\ell \text{ odd}); \qquad (1.5)$$

the integer $h(f; \mathfrak{l})$ appearing above is actually 0 if $f \in M_k(\Gamma_1(N))$, provided $\mathfrak{l} \nmid \mathcal{L}$ (actually a slightly stronger result holds, see Proposition 3.13). This may shed some light on the behaviour of $h(f; \mathfrak{l})$, which the authors in [5] comment as being rather mysterious, as ℓ varies. Apart from this, the point here is that our proofs are 'softer', however note that we do not get an asymptotic formula. We make some efforts in finding a constant $\mathcal{C}$ depending only on k, N such that (1.4) holds for all $\ell > \mathcal{C}$. The reader may look at Sect. 3.1. In fact it follows from Proposition 3.13 that $h(f; \mathfrak{l}) = 0$ for all $\ell > \mathcal{C}$ with suitable $\mathcal{C}$ as above, see Remark 3.14. More generally, as an outcome of our line of thought, in Proposition 3.15 we note that for those $f \in \widetilde{M}(N)$ which not constants mod $\mathfrak{l}$ and are finite linear combinations of eigenforms with pairwise distinct system of eigenvalues and are non-constant mod $\mathfrak{l}$, one would have $h(f; \mathfrak{l}) = 0$. We speculate that the converse to the previous statement is true as well and this is the content of Conjecture 3.16.

The reader may note that there is no contradiction with the examples in [5, 7] since e.g. the prime $\ell = 3$ considered there divides $\mathcal{L}$ (at level 1 and weight 24). See example 3.12 concerning $f = \Delta^2$ (Δ is Ramanujan's Delta function) for some more clarity on this. Moreover if the level N is square-free, we obtain results similar to (1.5) for the set $\pi_{\mathrm{sf}}(f, x; \mathfrak{l}) := \{n \leq x \mid n \text{ square-free}, a(f, n) \not\equiv 0 \bmod \mathfrak{l}\}$. Several such results are collected in Proposition 3.10. Finally let us mention that we briefly discuss an algebraic way to approach some of our results in Sect. 3.2.

In the second half of the paper (Sect. 4) we derive analogous results for Siegel modular forms. Let $F \in M_k^n(\Gamma_1(N))$ be a Siegel modular form with Fourier coefficients in the ring of integers $\mathcal{O}_K$ of a number field K. We first prove a statement which essentially says (see Theorem 4.4) that for $F \not\equiv 0 \bmod \mathfrak{l}$ as above, there exist infinitely many $\mathrm{GL}(n, \mathbf{Z})$-inequivalent 'primitive' matrices $T \in \Lambda_n$ such that the Fourier coefficients satisfy $a_F(T) \not\equiv 0 \bmod \mathfrak{l}$ at least for all primes ℓ large enough. This generalises a result of Yamana [27] who proved a similar result when $\ell = \infty$, showing the existence of at least one non-zero primitive Fourier coefficient. Our proof uses a refinement of a method (of descending to elliptic modular forms) presented in [9], some results on "oldforms mod $\mathfrak{l}$" on elliptic modular forms (Theorem 3.7), and the existence of a Sturm's bound for the space $M_k^n(\Gamma_1(N))$, which is formulated and proved in Proposition 4.1 generalising the level one result from [19].

Then we give lower bounds on the number of $d \le x$ such that $d = \det(2T)$ and that the Fourier coefficients $a_F(T) \not\equiv 0 \bmod \mathfrak{l}$ for some T (also satisfying additional arithmetic properties, see Theorem 4.9, Sect. 4). The proofs are based on reduction of the question to spaces of elliptic modular forms via the Fourier-Jacobi expansions, and using either the results from [4–6]; or sometimes using the lower bounds (cf. Sect. 3.3) from this paper. In particular (see Theorem 4.9 (b)) we show that the quantity $\Pi(x;\mathfrak{l}) = \pi_F(x, \det; \mathrm{sf})$ (cf. Sect. 4.1) defined by

$$\Pi(x;\mathfrak{l}) := \{d \le x \mid d \text{ square-free}, a_F(T) \not\equiv 0 \bmod \mathfrak{l} \text{ for some } T \in \Lambda_n^+ \text{ such that } \det(2T) = d\}$$

satisfies for all ℓ sufficiently large (see Remark 4.12) and any $\mathfrak{l}$ lying over ℓ, the lower bound

$$\#\Pi(x;\mathfrak{l}) \gg \frac{x}{(\log x)^{\beta(F;\mathfrak{l})}}, \qquad (n \text{ odd}) \tag{1.6}$$

for some constant $0 < \beta(F;\mathfrak{l}) \le 3/4$ where the implied constant depends on F and $\mathfrak{l}$. This was in fact our main motivation for writing this paper, and can be viewed as a mod $\mathfrak{l}$ version of the recent result [7, Theorem 1] on non-zero 'fundamental' Fourier coefficients of Siegel modular forms.

Finally let us mention that to obtain (1.6), we actually use its Archimedean analogue (only the existence of a nonvanishing fundamental Fourier coefficient) from [7] as an input. So we obtain no new proof of it, even though such a thing is desirable (a preliminary inspection shows that even then ℓ has to be large), and seems hard. Moreover since our results, say for $\Pi(x;\mathfrak{l})$, hold only for large enough ℓ, merely having $\Pi(x;\mathfrak{l}) > 0$ is a tautology as we can fix T such that $a_F(T) \neq 0$ and remove the finitely many ℓ such that $\ell \mid a_F(T)$. We therefore must at the least aim for a statement like $\Pi(x;\mathfrak{l}) \to \infty$ as $x \to \infty$. The same remark applies to the nonvanishing mod ℓ of primitive Fourier coefficients as well. Before closing this introduction, let us remark here that our method of treating Siegel modular forms may in principle work for Hermitian modular forms of arbitrary degree, however there should be several technicalities to be overcome.

Finally for the reader's convenience, let us mention that the only place where we use the results from [4–6] are in Theorem 4.9 and Proposition 4.14. Alongwith this in remark 4.10, we also use results from Sect. 3.2.1, precisely Theorem 3.7.

2. Setting and notation

Following standard notation, let $M_k(\Gamma_1(N))$ and $M_k^n(\Gamma_1(N))$ denote the space of elliptic (respectively Siegel) modular forms of weight k and level $\Gamma_1(N)$ (respectively $\Gamma_1^n(N)$). We denote their Fourier expansions as follows ($\mathbf{H}$ and $\mathbf{H}_n$ being the respective upper-half spaces):

$$f(\tau) = \sum_{n \geq 0} a(f, n) e(n\tau) \qquad (\tau \in \mathbf{H}, f \in M_k(\Gamma_1(N))) \tag{2.1}$$

$$F(Z) = \sum_{T \in \Lambda_n} a_F(T) e(TZ), \qquad (Z \in \mathbf{H}_n, F \in M_k^n(\Gamma_1(N))) \tag{2.2}$$

where $e(z) = \exp(2\pi i z)$ for $z \in \mathbf{C}$, $e(TZ) = e(\mathrm{trace}(TZ))$, Λ_n denotes the set of half-integral positive semi-definite symmetric matrices over $\mathbf{Z}$:

$$\Lambda_n := \{S = (s_{i,j}) \mid S = S^t, s_{i,i} \in \mathbf{Z}, s_{i,j} \in \frac{1}{2}\mathbf{Z}, \text{ and } S \text{ is positive semi-definite}\}.$$

Here and throughout we denote by A^t as the transpose of a matrix A. We also put Λ_n^+ to be the positive-definite elements of Λ_n. The corresponding spaces of cusp forms are denoted by $S_k(\Gamma_1(N))$ and $S_k^n(\Gamma_1(N))$. To avoid any confusion, let us mention that for this paper

$$\Gamma_1^n(N) := \{\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_n \mid \det(A) \equiv \det(D) \equiv 1 \bmod N, \ C \equiv 0 \bmod N\}.$$

Further, if $\mathcal{O}_K$ is the ring of integers of a number field K, we put

$$M_k^n(\Gamma_1(N))(\mathcal{O}_K) := \{F \in M_k^n(\Gamma_1(N)) \mid a_F(T) \in \mathcal{O}_K \text{ for all } T\}, \tag{2.3}$$

$$\widehat{M}_k(N, \mathcal{O}_K) := \{f \in M_k(\Gamma_1(N)) \mid a(f, n) \in \mathcal{O}_K \text{ for all } n \geq 1, a(f, 0) \in K\}. \tag{2.4}$$

We denote by $S_k(\Gamma_1(N))(\mathcal{O}_K)$, $S_k^n(\Gamma_1(N))(\mathcal{O}_K)$ to be the respective spaces of cusp forms.

For two positive functions on $\mathbf{R}$, we write $f(x) \asymp g(x)$ if there exist two positive constants c_1, c_2 such that $c_1 g(x) \leq f(x) \leq c_2 g(x)$ for all $x \geq 1$.

We now recall some notions about Fourier-Jacobi expansions of Siegel modular forms. We first recall that the content $c(T)$ for any matrix $T = (t_{i,j}) \in \Lambda_n$ is defined as gcd of all the t_{ii} and all the $2t_{i,j}$ with $i \neq j$. In particular, T is called primitive, if $c(T) = 1$.

For a fixed $S \in \Lambda_{n-1}^+$ we consider a Jacobi form $\varphi(\mathfrak{Z}) = \phi_S(\tau, z) e(SZ)$ (where $\mathfrak{Z} = \left(\begin{smallmatrix} \tau & z \\ z & Z \end{smallmatrix}\right) \in \mathbf{H}_n$) of index S on the group $\Gamma_1(N) \ltimes \mathbf{Z}^{n-1}$. Its theta expansion has the form

$$\phi_S(\tau, z) = \sum_{\mu_0} h_{\mu_0}(\tau) \Theta_S[\mu_0](\tau, z) \tag{2.5}$$

where μ_0 runs over $\mathbf{Z}^{n-1}/2S\mathbf{Z}^{n-1}$. We write the Fourier expansions of ϕ_S and h_{μ_0} as

$$\phi_S(\tau, z) = \sum_{r,\mu} b(r, \mu) e(r\tau + \mu^t \cdot z),$$

$$h_{\mu_0}(\tau) = \sum_{r} b(r, \mu_0) e\left((r - S^{-1}[\mu_0/2]) \cdot \tau\right) \tag{2.6}$$

with $r \in \mathbf{N}_0$, $\mu \in \mathbf{Z}^{(n-1,1)}$ and for all $L \in \mathbf{Z}^{(n-1,1)}$, note the following invariance property

$$b(r,\mu) = b(r + L^t \cdot \mu + S[L], \mu + 2S \cdot L). \tag{2.7}$$

Here $A[B] = A^t BA$ for matrices A, B of suitable sizes. We would be mainly interested in the Fourier-Jacobi expansion of $F \in M_k^n(\Gamma_1(N))$ of type $(1, n-1)$:

$$F(\mathfrak{Z}) = \sum_{S \in \Lambda_{n-1}} \phi_S(\tau, z) e(SZ) \qquad (\mathfrak{Z} = \left(\begin{smallmatrix} \tau & z \\ z & Z \end{smallmatrix}\right)); \tag{2.8}$$

then the ϕ_S are Jacobi forms in the above sense.

3. Elliptic modular forms

Let $f \in M_k(\Gamma_1(N))(\mathcal{O}_K)$. By the classical theory of newforms, there exist unique $\alpha_{i,\delta} \in \mathbf{C}$ such that $f(\tau)$ can be written as

$$f(\tau) = \sum_{i=1}^{s} \sum_{\delta | N} \alpha_{i,\delta} f_i(\delta \tau), \tag{3.1}$$

where $\{f_1, f_2, \ldots, f_s\}$ constitute a basis of newforms of weight k and level dividing N, including the Eisenstein-newforms. For the above statement see [17] for cusp forms, and [26] for an explicit description of Eisenstein series. In order to consider congruences mod $\mathfrak{l}$, we require that the scalars $\alpha_{i,\delta}$ in (3.1) are all $\mathfrak{l}$-integral. We would later prove that this is the case for suitable primes $\mathfrak{l}$, see Lemma 3.1. *We assume throughout this paper that* $k \geq 2$.

We note here that our normalisation for the Eisenstein newforms is that it's Fourier coefficient at $n = 1$ equals 1; for example in the case of level N new-Eisenstein series, given two primitive Dirichlet characters χ_1, χ_2 mod N with $\chi_1, \chi_2 = \chi$, $\chi(-1) = (-1)^k$, we consider the newforms

$$E_{\chi_1,\chi_2}(\tau) := \delta_{1,\chi_1} L(1-k, \chi_1) + \sum_{n \geq 1} \left(\sum_{d|n} \chi_1(n/d) \chi_2(d) d^{k-1} \right), \tag{3.2}$$

when $k \geq 3$. See [26] for more details. Here δ_{1,χ_1} is 1 or 0 according as χ_1 is principal or not. Moreover $L(s, \chi_1)$ is the Dirichlet L-function attached to χ_1. In the above notation, $E_{\chi_1,\chi_2} \in \widehat{M}_k(N, \mathcal{O}_K)$. Since we would be mostly interested in counting the number of non-zero Fourier coefficients $a(f, n)$ for $1 \leq n \leq x$, with a large parameter x, this choice of normalisation would be sufficient for our purpose.

We recall here the Sturm's bound for $M_k(\Gamma_1(N))$: if $G, H \in M_k(\Gamma_1(N))(\mathcal{O}_K)$ and satisfy $a(G, n) \equiv a(H, n) \bmod \mathfrak{l}$ for all

$$n \leq \mathcal{S}^1(k, N) := \frac{k}{12}[\mathrm{SL}(2, \mathbf{Z}) \colon \Gamma_1(N)], \tag{3.3}$$

modulo some prime $\mathfrak{l} \subset \mathcal{O}_K$, then $G \equiv H \bmod \mathfrak{l}$. Later we would write down a similar bound for Siegel modular forms. We would also require the Archimedian version of the Sturm's bound, and note that the bound in (3.3) also works in this case.

Recall from (1.2) *and* (3.2) *the Fourier expansion of the set of all newforms* $\{f_i\}$ *on* $\Gamma_1(N)$. *Throughout the paper, we assume without loss of generality that* K *contains the eigenvalues* $b_i(n)$ (*for all* i *and* $n \geq 1$) *and is Galois over* $\mathbf{Q}$. See Remark 3.11.

3.1. (Non)-congruences, analytic way

For our further requirements, we need to separate Hecke eigenvalues of two newforms mod $\mathfrak{l}$ in an efficient way (for suitable $\mathfrak{l}$). For this we first discuss an analytic way relying essentially on Deligne's bound. In the next subsection, we sketch a possible simple algebraic way to do this in certain special situations.

Let us now focus on (3.1). For all primes p and $1 \leq i \leq s$, one has $T_p f_i = b_i(p) f_i$ (f_i, b_i as in (1.2), T_p being the p-th Hecke operator on $\Gamma_1(N)$). By "strong multiplicity-one", if $i \neq j$, we can find infinitely many primes p *coprime to* N such that $b_i(p) \neq b_j(p)$. See [17, Theorem 4.6.19] for cusp forms and [26] for Eisenstein series. We would like to have a more precise mod $\mathfrak{l}$ version of this, with effective bounds on p.

Let us consider a set of primes $q_{i,j}$ all coprime to N such that for all $i \neq j$, one has $b_i(q_{i,j}) \neq b_j(q_{i,j})$ with $b_i(\cdot)$ as above. Let us define the non-zero quantity

$$\mathcal{L}(\{q_{i,j}\}; f) := \prod_{(i,j)\in S_f \times S_f}{}^{'} \big(b_i(q_{i,j}) - b_j(q_{i,j})\big) \tag{3.4}$$

where S_f is the set of indices i for which $f_i|B_\delta$ (for some $\delta|N$) appears in f (cf. (3.1)), i.e.,

$$S_f = \{1 \leq i \leq s \mid \alpha_{i,\delta} \neq 0 \text{ for some } \delta|N\}. \tag{3.5}$$

Moreover $\prod{}^{'}$ signifies that the product is over indices $i \neq j$.

We call any such set of primes $\{q_{i,j}\}$ ($i, j \in S_f$) as **admissible** for f. By strong multiplicity-one, there are infinitely many admissible sets for any f.

Lemma 3.1. *Let* $\{q_{i,j}\}$ *be any set of admissible primes for* f. *With the notation and setting as above, the* $\alpha_{i,\delta}$ *appearing in* (3.1) *are all* $\mathfrak{l}$*-integral for any prime* $\mathfrak{l} \subset \mathcal{O}_K$ *such that* $\mathfrak{l} \nmid \mathcal{L}(\{q_{i,j}\}; f)$.

We postpone the proof of the lemma until that of the next proposition. In fact the proof of the lemma follows the lines of that of Proposition 3.4 given below, and this explains our choice.

3.1.1. Ensuring non-congruences by using analytic estimates Recall our convention on K from the previous section. For an *arbitrary* prime q such that $b_i(q) \neq b_j(q)$ suppose now that there is a congruence

$$b_i(q) \equiv b_j(q) \bmod \mathfrak{l}. \tag{3.6}$$

For clarity of presentation let us assume here that $b_i(q), b_j(q)$ are the Fourier coefficients of two cuspidal newforms f_i, f_j. At the end of this subsection we consider the minor changes required to handle Eisenstein series. We would follow this convention in the subsequent subsections as well.

If we take norms on both sides of (3.6), we get a divisibility relation in $\mathbf{Z}$:

$$N_{K|\mathbf{Q}}(\mathfrak{l}) \mid N_{K|\mathbf{Q}}\left((b_i(q) - b_j(q))\right). \tag{3.7}$$

Let us recall Deligne's bound for the Fourier coefficients of a newform of level N:

$$|a(g,n)| \leq \sigma_0(n) n^{(k-1)/2} \qquad \left(\sigma_0(n) = \sum_{d|n} 1\right),$$

and Shimura's result about the existence of a basis of $S_k(\Gamma_1(N))$ with (rational) integral Fourier coefficients which implies that for any $\sigma \in Aut(\mathbf{C})$, $g^\sigma := \sum_n \sigma(a_g(n)) q^n \in S_k(\Gamma_1(N))$ whenever g is. Therefore by the triangle inequality we have for any prime q

$$|b_i(q) - b_j(q)| \leq 4q^{(k-1)/2} \tag{3.8}$$

and from the above, the same inequality as in (3.8) holds with the f_i replaced by f_i^σ for any σ in the Galois group of $K|\mathbf{Q}$.

We further let $\mathfrak{d} = [K : \mathbf{Q}]$ and $\mathfrak{h}$ to be the inertia degree of $\mathfrak{l}$ over ℓ. Therefore the validity of the congruence in (3.6) imples that

$$\ell^{\mathfrak{h}} = N_{K|\mathbf{Q}}(\mathfrak{l}) \leq (4q^{\frac{k-1}{2}})^{\mathfrak{d}}; \tag{3.9}$$

and equivalently that if $\ell > (4q^{\frac{k-1}{2}})^{\mathfrak{d}/\mathfrak{h}}$, then the congruences (3.6) cannot hold at q. In particular if we put $P := \max_{i \neq j} m_{i,j}$ with $m_{i,j}$ as in (1.3), then the condition

$$\ell > (4P^{\frac{k-1}{2}})^{\mathfrak{d}/\mathfrak{h}} \tag{3.10}$$

imples that $\mathfrak{l} \nmid \mathcal{L}$, where $\mathcal{L}$ is as in (1.3).

Now we briefly consider the cases if at least one of the f_i, f_j above is an Eisenstein newform. Analogous to (3.8), from (3.2) we see that in this case

$$|b_i(q) - b_j(q)| \leq 2(1 + q^{k-1}),$$

and by slight abuse of notation, using the same letter P, we see that $\mathfrak{l} \nmid \mathcal{L}$ provided

$$\ell > (2 + 2P^{k-1})^{\mathfrak{d}/\mathfrak{h}},$$

where $P = \max_{i \neq j} m_{i,j}$.

In the next subsection we show how to bound the $m_{i,j}$ in a slightly more general situation.

3.1.2. Effective bounds for the $m_{i,j}$ and ensuring $\mathfrak{l} \nmid \mathcal{L}(\{m_{i,j}\}; f)$ For future applications, we need to choose primes $\{q_{i,j}\}$ separating the newforms $\{f_j\}$ such that $(q_{i,j}, 2NQ) = 1$, where Q is an arbitrary given integer. We would first bound the elements of the "smallest" such admissible set of primes (each coprime to a fixed integer M) in terms of k, N, M, and then provide a constant $\mathcal{C} = \mathcal{C}(k, N, M)$ such that for all $\ell > \mathcal{C}$ and all $\mathfrak{l} \mid \ell$, one has $\mathfrak{l} \nmid L(\{q_{i,j}\}; f)$.

To this end we consider as before, for any $f_i \in \{f_1, \ldots, f_s\}$ and for any given $M \geq 1$ containing all the prime factors of N, the modified modular form

$$f_i^{(M)}(\tau) = \sum_{n\geq 1} \mathbf{b}_i(n)q^n := \sum_{(n,M)=1} b_i(n)q^n \in M_k(\Gamma_1(\widetilde{M})), \tag{3.11}$$

where $\widetilde{M} = N^2$ if $M = N$, and NM^2 otherwise. Observe that all of the $f_i^{(M)}$ are non-zero and moreover that $f_i^{(M)} \neq f_j^{(M)}$ whenever $i \neq j$. Now there are two cases, and our treatment would be slightly different in each case.

We record here a lemma about bounding the smallest prime p such that for two distinct newforms f, g on $M_k(\Gamma_1(N))$, one has $a(f, p) \neq a(g, p)$.

Proposition 3.2. *Let f_i, f_j, M be as above and $i \neq j$. Let $\mathbf{m}_{i,j}$ be the smallest prime p coprime to M such that $b_i(p) \neq b_j(p)$. Then for any given $\epsilon > 0$ there exist $c_\epsilon > 0$ depending only on ϵ and absolute constants $c, c' > 0$ such that*

$$\mathbf{m}_{i,j} \leq \mathcal{H}(k, \widetilde{M}) := \begin{cases} c_\epsilon \widetilde{M}^\epsilon k^{1+\epsilon} N^{3/2+\epsilon} & \textit{if } f_i, f_j \textit{ are cuspidal}, \\ c\widetilde{M} & \textit{if only one of them is cuspidal}, \\ c'\widetilde{M} & \textit{if both are non-cuspidal}. \end{cases} \tag{3.12}$$

Proof. For the case of cusp forms see [2, (2.14, and proof of Prop. 2.1)] and [13, Remark following Prop. 5.22, p. 118]. The basic idea is that if $b_i(p) = b_j(p)$ for all primes $p \leq x$ which are coprime to an integer D, then by multiplicativity one has $b_i(n) = b_j(n)$ for all square-free $n \leq x$ coprime to D. Therefore on the one hand for any smooth compactly supported function ω, we find that

$$0 = \sum_n |b_i(n)|^2\omega(n/x) - \sum_n b_i(n)\overline{b_j(n)}\omega(n/x), \tag{3.13}$$

where the summation is over square-free integers $\leq X$ which are coprime to M. On the other hand, by applying a modified version of the Rankin-Selberg method to $f_i \otimes \overline{f_i}$ and $f_i \otimes \overline{f_j}$ $(i \neq j)$ respectively, the asymptotic properties of the first and second sums allows us to finish the proof. For the convenience of the reader, let us give some more details of this argument.

We follow [2, proof of Prop. 2.1)]. Namely, analogously to [2, (2.6)] we start with

$$L^\flat(f_i \times \overline{f_j}, s) := \sideset{}{^\#}\sum_{n\geq 1,\, (n,\widetilde{M})=1} b_i(n)\overline{b_j(n)}n^{-s} = \prod_{p\nmid \widetilde{M}} (1 + b_i(p)\overline{b_j(p)}p^{-s}), \tag{3.14}$$

where $\sum^{\sharp}$ signifies sum over square-free integers. The successive definitions and calculations can now be obviously modified – replacing 'N' by $\widetilde{M}$ wherever relevant: we do not repeat them here. We remark that the Dirichlet series H_1 (loc. cit.) remains the same, and H (loc. cit.)) will be given by an Euler product away from $\widetilde{M}$. Finally the lower bound of $H(1)$ should be in our case (for any $\epsilon > 0$) $H(1) \gg_{\epsilon} \widetilde{M}^{-\epsilon}$. Rest of the bounds remain the same as in [2, (2.12)]. We note the final outcome. Taking $c = 1/2 + \epsilon$ (loc. cit.) for all $x > 0$, one arrives at the following asymptotic formula:

$$\sum_{n\geq 1,\,(n,\widetilde{M})=1}^{\#} b_i(n)\overline{b_j(n)}\omega(n/x) = \delta(f_i, \overline{f_j})C(f_i, \omega)x + O(x^{1/2+\epsilon}k^{1/2+\epsilon}N^{\frac{3}{4}+\epsilon}), \tag{3.15}$$

where $\delta(\cdot,\cdot)$ is the Kronecker's delta function, $C(f_i, \omega)$ a positive constant as defined in [2]. It is now easy to derive from (3.15) an upper bound for x so that (3.13) cannot hold.

The second case is easy to deal with; and we only mention a prototype example when $k \geq 3$. Namely if $f_i = E_{\chi_1,\chi_2}$ and $f_j = g$ (g a cuspidal newform), then the inequalities

$$|\chi_1(p) + \chi_2(p)p^{k-1}| \geq p^{k-1} - 1 > 2p^{(k-1)/2}$$

hold for any $p \nmid N$ provided $p \geq 9$ say. Therefore the smallest prime such that $9 \leq p < M$ does the job if $M > 9$, since by Deligne's bound we have $|a(g, p)| \leq 2p^{(k-1)/2}$. A very crude bound for all values of M is $p \ll M$.

The remaining case is handled very similarly and we give a prototype example. Let $f_i = E_{\chi_1,\chi_2}$, $f_j = E_{\psi_1,\psi_2}$. If $\chi_1 = \psi_1$ or $\chi_2 = \psi_2$, clearly any prime $p \leq M$, $p \nmid M$ works. Otherwise suppose one has for $p \nmid N$

$$p^{k-1}(\chi_2(p) - \psi_2(p)) = \psi_1(p) - \chi_1(p) \neq 0. \tag{3.16}$$

Now $\chi_j(p)$, $\psi_j(p)$ are $\phi(N)$-th roots of unity, and so are their Galois conjugates. Consider the above equation in the cyclotomic field $\mathbf{Q}(\zeta_{\phi(N)})$ where ζ_m is a primitive m-th root of unity. If we take norms to $\mathbf{Q}$ in (3.16) and note that $|N(\chi_2(p) - \psi_2(p))| \geq 1$ we get (putting $T = [\mathbf{Q}(\zeta_{\phi(N)})\colon \mathbf{Q}]$)

$$p^{(k-1)T} \leq 2^T, \qquad \text{or } p^{k-1} \leq 2,$$

which forces $p = 2$ if $k = 2$ and a contradiction otherwise. Thus a very crude bound for such p is $p \ll M$. □

Remark 3.3. If we are concerned with the spaces $M_k(N, \chi)$ for a fixed χ instead of $M_k(\Gamma_1(N))$, a much simpler argument about the effective separation of newforms by finitely many primes could be given by using multiplicativity and Sturm's bound as in (3.3). This is because in this case $b_i(p) = b_j(p)$ implies that $b_i(p^m) = b_j(p^m)$ for all $m \geq 1$. This is not necessarily true on $\Gamma_1(N)$.

(A) *Not necessarily distinct primes*

We want to choose primes $q_{i,j}$ such that for all $i \neq j$,

$$b_i(q_{i,j}) \not\equiv b_j(q_{i,j}) \bmod \mathfrak{l} \tag{3.17}$$

and $(q_{i,j}, M) = 1$. We simply choose the $\mathbf{m}_{i,j}$ to be the smallest prime (necessarily less or equal to the quantity $\mathcal{H}(k, \widetilde{M})$) such that $\mathbf{b}_i(\mathbf{m}_{i,j}) \neq \mathbf{b}_j(\mathbf{m}_{i,j})$ and then choose $\mathfrak{l}$ such that $\mathfrak{l} \nmid \mathcal{L}^{(M)}(\{\mathbf{m}_{i,j}\}; f)$ where (recall S_f from (3.5))

$$\mathcal{L}^{(M)}(\{\mathbf{m}_{i,j}\}; f) := \prod_{i,j \in S_f \times S_f}{}^{'} \left(b_i(\mathbf{m}_{i,j}) - b_j(\mathbf{m}_{i,j})\right). \tag{3.18}$$

Note that in particular $\max_{i,j}\{\mathbf{m}_{i,j}\} \leq \mathcal{H}(k, \widetilde{M})$ and from our definition (3.11), necessarily $(\mathbf{m}_{i,j}, M) = 1$.

Now by the arguments in Sect. 3.1.1 we see that the following ℓ (and any $\mathfrak{l} \mid \ell$) work:

$$\ell > \left(4\mathcal{H}(k, \widetilde{M})^{s(s-1)(k-1)/4}\right)^{\mathfrak{d}/\mathfrak{h}}. \tag{3.19}$$

In particular when $M = N$, by our choice we have $\mathbf{m}_{i,j} = m_{i,j}$ (cf. (1.3)) and thus an effective upper bound for $\mathcal{L}(\{m_{i,j}\}; f)$.

(B) *Distinct primes* If we insist that the primes $q_{i,j}$ requested as above are also pairwise distinct, we can proceed similarly as in (A) with some modifications.

We start by picking the prime $p_{1,2} := \mathbf{m}_{1,2}$ coprime to M from an admissible set for f as in (A) above. We then reiterate this procedure as follows. Next we consider the forms $f_1^{(Mp_{1,2})}$ and $f_3^{(Mp_{1,2})}$ (both are non-zero modular forms) and find a prime $p_{1,3} \leq \mathcal{H}(k, NM^2p_{1,2}^2)$ such that $b_1(q) \not\equiv b_3(q) \bmod \mathfrak{l}$ and $(p_{1,3}, Mp_{1,2}) = 1$. We carry on this procedure to get primes $p_{1,j}$ $(2 \leq j \leq s)$ satisfying $(p_{1,j}, Mp_{1,2} \cdots p_{1,j-1}) = 1$. We finally do this for the indices other than 1 and find that $\max_{i,j}\{p_{i,j}\} \ll \mathfrak{S}(k, N, M)$, where

$$\mathfrak{S}(k, N, M) = \mathcal{H}(k, NM^2 \prod_{i<j} p_{i,j}^2), \quad p_{i,j} \leq \mathcal{H}(k, NM^2 \prod_{i<t<j} p_{i,t}^2). \tag{3.20}$$

We thus consider $\mathfrak{l} \nmid \mathcal{L}_{\mathrm{sf}}^{(M)}(\{p_{i,j}\}; f)$ where

$$\mathcal{L}_{\mathrm{sf}}^{(M)}(\{p_{i,j}\}; f) := \prod_{i,j \in S_f \times S_f}{}^{'} \left(b_i(p_{i,j}) - b_j(p_{i,j})\right). \tag{3.21}$$

If $M = 1$, we omit it from the notation.

By using Deligne's bound we again deduce that if

$$\ell > (4\mathfrak{S}(k, N, M)^{\frac{s(s-1)(k-1)}{4}})^{\mathfrak{d}/\mathfrak{h}}, \tag{3.22}$$

none of the congruences $b_i(p_{i,j}) \equiv b_j(p_{i,j}) \bmod \mathfrak{l}$ in particular hold for $i \neq j$ where $(p_{i,j}, M) = 1$ and $p_{i,j}$ are pairwise distinct.

We can now state the main workhorse of this paper. For suitable prime ideals $\mathfrak{l}$, if f is not a constant $\bmod\ \mathfrak{l}$ we show that by considering the Hecke module generated by f one can extract a newform $\mathfrak{g}$ ocurring in f, such that the Fourier coefficients of $\mathfrak{g}$ are integral linear combinations of those of f. This would allow us to reduce our nonvanishing questions to those about newforms mod $\mathfrak{l}$. Also from the point of view of this paper, as we discussed before, modular forms which are constant mod $\mathfrak{l}$ play no role and thus should be avoided.

Proposition 3.4. *Let f be as in (3.1) and let $Q \geq 1$ be arbitrary. Let $\{q_{i,j}\}$ be a set of admissible primes for f such that $(q_{i,j}, QN) = 1$. Then there exists a newform $\mathfrak{g}$ of level dividing N such that one has the relation*

$$a(\mathfrak{g}, \mathfrak{n}) \equiv \sum_{t|N} \beta_t a(f, \gamma_t \Delta \mathfrak{n}) \bmod \mathfrak{l} \tag{3.23}$$

for all $\mathfrak{n} \geq 1$ such that $(\mathfrak{n}, QN) = 1$, for some $\Delta | N$; for some β_t which are $\mathfrak{l}$-integral; and where

(a) $\gamma_t \in \mathbf{Q}$ *are all square-free with* $(\gamma_t, QN) = 1$ *provided* $\mathfrak{l} \nmid \mathcal{L}_{\mathrm{sf}}^{(QN)}(\{q_{i,j}\}; f)$ and f *is not constant* mod $\mathfrak{l}$*;*
(b) $\gamma_t \in \mathbf{Q}$ *with* $(\gamma_t, QN) = 1$ *provided* $\mathfrak{l} \nmid \mathcal{L}^{(QN)}(\{q_{i,j}\}; f)$ and f *is not constant* mod $\mathfrak{l}$.

Note that the set $\{p_{i,j}\}$ constructed in Sect. 3.1.2 (B) above satisfy the properties requested for the admissible set in (a). Similarly the set $\{\mathbf{m}_{i,j}\}$ is an example for the admissible sets in (b).

Proof. For ease of notation, in (a) let us assume without loss of generality that the admissible set is $\{p_{i,j}\}$. Also we put $\mathcal{L}_1 := \mathcal{L}_{\mathrm{sf}}^{(QN)}(\{p_{i,j}\}; f)$ and $\mathcal{L}_2 := \mathcal{L}^{(QN)}(\{q_{i,j}\}; f)$.

We start from (3.1). To talk about congruences, we need that all the $\alpha_{i,\delta}$ are $\mathfrak{l}$-integral under the hypotheses on $\mathfrak{l}$. This is guarranteed by Lemma 3.1. By our assumption on f, not all of the $\alpha_{i,\delta}$ can be $\equiv 0 \bmod \mathfrak{l}$. We may, after renumbering the indices, assume $\alpha_{1,\delta} \not\equiv 0 \bmod \mathfrak{l}$ for some $\delta | N$. Let $q := p_{1,2}$ or $q := q_{1,2}$ according as we are in case (a) or (b) be the prime chosen as before (see the discussion preceeding this theorem) for which $b_1(q) \not\equiv b_2(q) \bmod \mathfrak{l}$. Note that $p_{1,2} \nmid QN$, $q_{1,2} \nmid QN$. Then consider the form $g_1(\tau) = \sum_{n=1}^{\infty} a_1(n) q^n := T(q) f(\tau) - b_2(q) f(\tau)$ so that

$$g_1(\tau) = \sum_{i=1}^{s} (b_i(q) - b_2(q)) \sum_{\delta|N} \alpha_{i,\delta} f_i(\delta\tau).$$

The modular forms $f_2(\delta\tau)$ for any $\delta | N$, do not appear in the decomposition of $g_1(\tau)$ but $f_1(\delta\tau)$ does for some $\delta | N$. Proceeding inductively in this way, we can remove all the non-zero newform components $f_i(\delta\tau)$ for all $i = 2, ..., s$ one by one, to obtain a modular form F $(= g_{|S_f|-1}$ in the above inductive procedure) in $M_k(\Gamma_1(N))$ such that on the one hand, we have

$$F(\tau) = \sum_{n=1}^{\infty} A(n) q^n := \prod_{2 \leq j \leq s} (b_1(p_{1,j}) - b_j(p_{1,j})) \sum_{\delta|N} \alpha_{1,\delta} f_1(\delta\tau). \tag{3.24}$$

By the construction of admissible sets, the product in (3.24) is $\not\equiv 0 \bmod \mathfrak{l}$, provided $\mathfrak{l} \nmid \mathcal{L}_1$ or $\mathfrak{l} \nmid \mathcal{L}_2$ according as we are in case (a) or (b). Therefore rescaling F, and calling the resulting function again as F, we on the other hand note that the inductive procedure gives us finitely many algebraic numbers β_t (polynomials in the $p_{i,j}$'s or the $q_{i,j}$'s and Dirichlet characters) and positive rational numbers γ_t (which quotients of the $p_{i,j}$'s or the $q_{i,j}$'s) such that for every n

$$A(n) = \sum_{\delta | N} \alpha_{1,\delta} b_1(n/\delta) \equiv \sum_t \beta_t a(f, \gamma_t n) \bmod \mathfrak{l}. \tag{3.25}$$

Let δ_1 be the smallest divisor of N such that $\alpha_{1,\delta_1} \not\equiv 0 \bmod \mathfrak{l}$ in (3.25). Then choosing $n = \mathfrak{n}\delta_1$ in (3.25) such that $(\mathfrak{n}, QN) = 1$, we get

$$\alpha_{1,\delta_1} b_1(\mathfrak{n}) \equiv \sum_t \beta_t a(f, \gamma_t \delta_1 \mathfrak{n}) \bmod \mathfrak{l} \tag{3.26}$$

as desired. The square-freeness of γ_t in part (a) follows from the pairwise distinctness of the $p_{i,j}$ (cf. Sect. 3.1.2 (B) preceeding this theorem, and from the formula for the action of Hecke operators at primes). This completes the proof. $\square$

Remark 3.5. It is obvious from the above proof that we do not really need all the primes $q_{i,j}$ from an admissible set for f to make the proof work. Only primes $q_{i_0,j}$ with $j \neq i_0$ (eg. we assumed $i_0 = 1$ in the above proof) for some fixed i_0 such that $\alpha_{i_0,\cdot} \not\equiv 0 \bmod \mathfrak{l}$ are required. Accordingly one could have modified the definition of $\mathcal{L}(\cdots)$. We do not do this to avoid additional notational burden. However in practice, this is what should be done.

Proof of Lemma 3.1. The method or idea of the proof (not the proof itself) is inspired from the proof of Theorem 3.7, if we take $\ell = \infty$ (see [1]). We follow it in principle, indicating suitable changes. Namely we start with $\alpha_{i,\delta} \in \mathbf{C}$ in (3.1). If i is an index for which $\alpha_{i,\delta} \neq 0$ (for some δ) we carry out the procedure of removing the newforms one by one, we would arrive at (3.26) corresponding to i. Here we choose δ_1 to be the minimum such that $\alpha_{i,\delta_1} \neq 0$ (not mod $\mathfrak{l}$!). Then choosing $n = \delta_1$ in (3.26) shows that $\alpha_{i,\delta_1} \cdot \prod_{2 \leq j \leq s, j \neq i} (b_1(q_{i,j}) - b_j(q_{i,j}))$ is an algebraic integer (in fact in $\mathcal{O}_K$). Note that the product appears since we had normalised F by this factor in the proof of Proposition 3.4. Thus by the definition of an admissible set, if $\mathfrak{l} \nmid \mathcal{L}(\{q_{i,j}\}; f)$ (in particular if ℓ is large enough, cf. section 3.1.1) $\alpha_{i,\delta}$ will be $\mathfrak{l}$-integral. Then inductively, we can ensure that all the $\alpha_{i,\delta}$ are $\mathfrak{l}$-integral. Since i was arbitrary, we get the lemma. $\square$

Remark 3.6. We point out another way of proving Lemma 3.1 by using some arguments from [16, proof of Lemma 2.1]. Working with the Sturm's bound for $M_k(\Gamma_1(N))$ (see (3.3)) as in our proof, this boils down to ensuring that $\nu_\ell(\det(b_{i,t}(n_j))) = 0$; where $f_i(t\tau) = \sum_n b_{i,t}(n) q^n$ with $\{f_i\}$ is the set of all newforms in $M_k(\Gamma_1(N))$ of level dividing N, and for each such i, $t = t(i)$ runs over divisors of $N/\text{level}(f_i)$. Moreover $\{n_j\}$ are certain indices less than the Sturm's bound for $M_k(\Gamma_1(N))$. It is however not clear how one can ensure that $\nu_\ell(\cdots) = 0$ without using 'analytic' inputs as in our paper, it does not help that we do not have much control on the set $\{n_j\}$ from [16]. If analytic inputs are used, then the ensuing bound on ℓ would be similar to ours.

3.2. (Non)-Congruences, algebraic way

There is of course an algebraic way to ensure non-congruences. Even though we would not really use this in the sequel (since we face some trouble, see below), except for some examples, we include this for completeness and possible further interest.

For each $1 \leq i \leq s$, from [12] let $c(f_i)$ denote the number whose square (which is in $\mathbf{Z}$) determines the congruence primes for f_i. **We assume that the Galois-orbits of each f_i is singleton** (i.e. f_i has Fourier coefficients in $\mathbf{Z}$). We note that $c(f_i)$ is closely related to the adjoint L-value $L(1, Ad(f_i))$, and there is the principle: "the prime factors of the denominators of the adjoint L-value give the congruence primes of f_i". This is proved in the seminal papers [11,12,20]. Let us put

$$\mathcal{C}(k, N) = \mathrm{lcm}\{c^2(f_1), \ldots, c^2(f_s)\}. \tag{3.27}$$

Then from the aforementioned references, for any prime

$$\ell \nmid 6N\mathcal{C}(k, N) \text{ such that } \ell \geq k, \tag{3.28}$$

one can ensure that for all $i \neq j$, and all $\mathfrak{L}$ lying over such ℓ in $\overline{\mathbf{Z}}$,

$$f_i \not\equiv f_j \bmod \mathfrak{L}. \tag{3.29}$$

This will imply the existence of a prime q with $b_i(q) \not\equiv b_i(q) \bmod \mathfrak{L}$, and **let us assume** $(q, N) = 1$. We do not know how to remove the assumption on Galois-orbits algebraically. However when $k = 2$, there are results by Ventosa ([25, Lem. 2.10.1]) which say that if a newform g is congruent to one of it's Galois-conjugates, then the congruence prime must divide the discriminant of the polynomial $Q_{g,p}(X) = \prod_\sigma (X - \sigma(a(g, p)))$ for any prime $p \nmid N\ell$. So in this case we would be able to produce admissible sets based on the remarks above, and therefore our method would work for all $\ell \geq k$ and $\ell \nmid$ (some fixed integer).

3.2.1. An application of Proposition 3.4 to oldforms mod $\mathfrak{l}$ Proposition 3.4 has many consequences, which we now discuss in the next couple of results. The first one is a statement about "oldform theory mod $\mathfrak{l}$". Let $f \in M_k(\Gamma_1(N))(\mathcal{O}_K)$ and $\mathfrak{l} \mid \ell$. Consider any admissible set $\{q_{i,j}\}$ whose elements are coprime to $M = QN$. The admissible set $\{\mathbf{m}_{i,j}\}$ from section 3.1.2 (A) is an example.

Theorem 3.7. *Let f be as above and suppose that f is not constant* mod $\mathfrak{l}$. *Let $Q \geq 1$ be given. Assume that $\mathfrak{l} \nmid \mathcal{L}^{(QN)}(\{q_{i,j}\}; f)$ for any admissible set $\{q_{i,j}\}$ such that $(q_{i,j}, QN) = 1$. Also assume $\ell > 2$. Then the following hold.*

(a) *If $(Q, N) = 1$, there exists infinitely many integers $n \geq 1$ such that $a(f, n) \not\equiv 0 \bmod \mathfrak{l}$ and $(n, Q) = 1$.*
(b) *If $(Q, N) > 1$, and we request that the f is not congruent* mod $\mathfrak{l}$ *to an $\mathfrak{l}$-integral linear combination of modular forms $g|B_{M_g}$ for some $g \in \widehat{M}_k(N, \mathcal{O}_K)$ (notation as in (2.4)) of level M_g dividing (Q, N) and $M_g > 1$; the same conclusion as in (a) above holds. (Here $g|B_{M_g}(\tau) = g(M_g\tau)$.)*

Note that when f is a cusp form, Theorem 3.7 is a generalisation mod $\mathfrak{l}$ of the classical oldform theory over $\mathbf{C}$ for all but finitely many ℓ.

Proof. For the proof we have to go back to (3.23) in Proposition 3.4. It is easy to see that since ℓ is odd there are infinitely many primes p with $(p, QN) = 1$, such that $b_1(p) \not\equiv 0 \bmod \mathfrak{l}$. This follows from the fact the set of primes such that $b_1(p) \equiv 0 \bmod \mathfrak{l}$ is 'Frobenian' of density which is positive but less than 1 (see [23, cf. proof of `Théorème 4.7` $(\mathtt{ii}_1)$ on p. 13]).

Therefore if $(Q, N) = 1$, in (3.23) we see that there exists t such that $n = \gamma_t \Delta \mathfrak{n}$ is coprime to Q and $a(f, n) \not\equiv 0 \bmod \mathfrak{l}$. This proves part (a).

If $(Q, N) > 1$ and the condition in the statement of part (b) is satisfied, this will imply that in (3.1) $\alpha_{i,1} \not\equiv 0 \bmod \mathfrak{l}$ for at least one $1 \le i \le s$, say $i = i(0)$. Then we would remove all the newforms except $f_{i(0)}$ and arrive at (3.26). However now, we can choose $\delta_1 = 1$ in (3.26) and hence we get part (b). □

Remark 3.8. It follows from the above proof that if the level N is square-free, then in Theorem 3.7 we can ensure that n is also square-free, for $\mathfrak{l}$ as in the theorem.

Of course Theorem 3.7 can be rephrased as a mod $\mathfrak{l}$ version of the familiar result in oldform theory for elliptic modular forms over $\mathbf{C}$.

Corollary 3.9. *Let f and ℓ be as in Theorem 3.7. Suppose that for some $Q \ge 1$, $a(f, n) \equiv 0 \bmod \mathfrak{l}$ for all n with $(n, Q) = 1$. Then f is constant* mod $\mathfrak{l}$ *if $(Q, N) = 1$, otherwise f is "old"* mod $\mathfrak{l}$*; i.e., there exist primes $\ell_1, \ldots, \ell_m$ such that $\ell_j | (Q, N)$ and $f \equiv \sum_j \alpha_j h_j | B_{\ell_j}$* mod $\mathfrak{l}$ *for some $h_j \in \widehat{M}_k(\Gamma_1(N_j))$, where $\ell_j N_j | N$, and α_j being $\mathfrak{l}$ integral.*

3.3. Quantitative results: elliptic modular forms

In [5] (resp. [6]) an asymptotic formula (resp. a lower bound) for the number of mod ℓ-non-zero Fourier coefficients of modular forms of integral (resp. half-integral) weights of level N was obtained. Following the notation in [5] let us define for $f \in M_k(\Gamma_1(N))(\mathcal{O}_K)$ which is not constant mod $\mathfrak{l}$, the counting function $\pi(f, x; \mathfrak{l})$ by

$$\pi(f, x; \mathfrak{l}) := \{n \le x | a(f, n) \not\equiv 0 \bmod \mathfrak{l}\};$$
$$\pi_Q(f, x; \mathfrak{l}) := \{n \le x, (n, Q) = 1 | a(f, n) \not\equiv 0 \bmod \mathfrak{l}\},$$
$$\pi_{\mathrm{sf}}(f, x; \mathfrak{l}) := \{n \le x | n \text{ square-free}, \ a(f, n) \not\equiv 0 \bmod \mathfrak{l}\},$$

and $\pi_{\mathrm{sf},Q}(f, x; \mathfrak{l})$ defined analogously.

Here we want to show quite elementarily using Proposition 3.4 that one can at least obtain upper and lower bounds of same order of magnitude for the quantities $\pi(f, x; \mathfrak{l})$ and $\pi_{\mathrm{sf}}(f, x; \mathfrak{l})$, however for $f \in M_k(\Gamma_1(N))$ of fixed weight and level. Similar considerations already seem to appear in [4]. These results in turn imply elementarily analogous results for Siegel modular forms.

Let $\{q_{i,j}\}$ be an admissible set for f and recall the admissible set $\{p_{i,j}\}$ constructed in Sect. 3.1.2 (B). We define the integers $P := \prod_{i,j} q_{i,j}$ and $U = \prod_{i \ne j} p_{i,j}$, $(i, j \in S_f)$.

Proposition 3.10. *Let the setting be as above and ℓ be odd. Then*

$$|\pi(f,x;\mathfrak{l})| \asymp \frac{x}{(\log x)^{\alpha(f)}} \quad (N \geq 1, \mathfrak{l} \nmid \mathcal{L}(\{q_{i,j}\};f)); \tag{3.30}$$

$$|\pi_{\mathrm{sf}}(f,x;\mathfrak{l})| \asymp \frac{x}{(\log x)^{\alpha(f)}}, \quad (N \textit{ square-free}, \mathfrak{l} \nmid \mathcal{L}_{\mathrm{sf}}(\{p_{i,j}\};f)). \tag{3.31}$$

The implied constants depend only on k, N, P, U, and $0 < \alpha(f) \leq 3/4$.

Remark 3.11. Note that we assumed K to be a bit large – containing the field L generated by all the eigenvalues of newforms of level dividing N. However this is just for notational convenience; one could have passed to the normal closure, say $\widetilde{K}$ of KL and noted that $\pi(f,x;\mathfrak{B}) = \pi(f,x;\mathfrak{l})$ for any $\mathfrak{B} \in \widetilde{K}$ lying over $\mathfrak{l}$.

Proof. We start from (3.23) in Proposition 3.4 in the special case when $Q = 1$. On the left hand side of (3.23) we get hold of a newform $\mathfrak{g}$ of level dividing N. For each $\mathfrak{n}$ such that $(\mathfrak{n}, N) = 1$ and $a(\mathfrak{g},\mathfrak{n}) \not\equiv 0 \bmod \mathfrak{l}$, from (3.23) there exists a $t \mid N$ such that $\beta_t a(f, \mathfrak{n}\gamma_t\Delta) \not\equiv 0 \bmod \mathfrak{l}$. Choose the smallest such t, call it $t(\mathfrak{n})$. Then the map

$$\pi_{PN\ell}(\mathfrak{g},x;\mathfrak{l}) \longrightarrow \pi(f,PNx;\mathfrak{l}), \quad \mathfrak{n} \mapsto \gamma_{t(\mathfrak{n})}\Delta\mathfrak{n},$$

where $P = \prod_{i,j} q_{i,j}$ as recalled above, is clearly injective since $\mathfrak{n}$ is away from PN. Note that $\gamma_{t(\mathfrak{n})}$, in this case, is a polynomial in the $p_{i,j}$'s. Therefore for all $x \geq 1$,

$$\#\pi_{PN\ell}(\mathfrak{g},x;\mathfrak{l}) \leq \#\pi(f,PNx;\mathfrak{l}); \tag{3.32}$$

and the lower bound in (3.30) then follows from (3.32) and from results of Serre [23, (4.6)] (note that ℓ is odd) for newforms. Indeed, if either

Clearly Serre's asymptotic formulae for $\pi_{PN\ell}(\mathfrak{g},x;\mathfrak{l})$ also hold if we omit finitely many primes from the ensemble that he starts with (loc. cit.). More precisely from [23], via the Galois representation attached with $\mathfrak{g}$, the primes $p \nmid N\ell$ are "Frobenian" and has analytic density $\alpha(\mathfrak{g})$ with $0 < \alpha(\mathfrak{g}) \leq 3/4$ (cf. [23, (6.3)]); and Serre shows that from this one can, using analytic techniques, give an asymptotic formula for $\pi_{N\ell}(\mathfrak{g},x;\mathfrak{l})$. For us, we additionally need omit the primes dividing P. Since the asymptotic formula depends only on the density of primes concerned, our claim holds true. We take $\alpha(f) := \alpha(\mathfrak{g})$.

For the upper bounds, we look instead at (3.1) and apply the same argument just presented. Here we consider the map $\mathfrak{n} \mapsto (\{i(\mathfrak{n}), \delta(\mathfrak{n})\}, \mathfrak{n}/\delta(\mathfrak{n}))$ where $i(\mathfrak{n})$ is the smallest index i for which $\alpha_{i,\delta}a(f_i|B_\delta,\mathfrak{n}) \not\equiv 0 \bmod \mathfrak{l}$ for some $\delta | N$ in (3.23) and once $i(\mathfrak{n})$ has been chosen, $\delta(\mathfrak{n})$ is the smallest divisor of N such that $\alpha_{i(\mathfrak{n}),\delta(\mathfrak{n})}a(f_{i(\mathfrak{n})}|B_{\delta(\mathfrak{n})},\mathfrak{n}) \not\equiv 0 \bmod \mathfrak{l}$. This is clearly an injective map, whence

$$\pi(f,x;\mathfrak{l}) \hookrightarrow \amalg_{i,\delta}\pi(f_i|B_\delta,x;\mathfrak{l}),$$

$\amalg$ being the *disjoint* union. We get

$$\begin{aligned}\#\pi(f,x;\mathfrak{l}) &\leq \sum_{i,\delta} \#\pi(f_i|B_\delta,x;\mathfrak{l}) \\ &\leq \dim M_k(\Gamma_1(N)) \cdot \max_{i,\delta}\{\#\pi(f_i|B_\delta,x;\mathfrak{l})\} \ll \max_i\{\#\pi(f_i,x;\mathfrak{l})\}\end{aligned}$$

and again results of Serre from [23] (cf. (1.1)) does the job.

Moreover if N is square-free, the above argument also works almost verbatim for $\pi_{\mathrm{sf}}(f, x; \mathfrak{l})$. In this case we have the additional information:

(i) Δ is square-free,
(ii) all the γ_t appearing in Proposition 3.4 are square-free rational numbers such that $(\gamma_t, N) = 1$ (so that if $\mathfrak{n}$ is square free and $(\mathfrak{n}, \gamma_t N) = 1$, $\gamma_{t(\mathfrak{n})}\Delta\mathfrak{n}$ is also square-free in (3.32)), and
(iii) Serre's asymptotic results clearly hold when we count over square-free integers as well. By this we mean an asymptotic formula of the form

$$\pi_{\mathrm{sf},UN\ell}(\mathfrak{g}, x; \mathfrak{l}) \sim c_{f;\mathfrak{l}} \frac{x}{(\log x)^{\alpha(f;\mathfrak{l})}} \qquad (\mathfrak{g} \text{ newform}) \tag{3.33}$$

for some constants $c_{f;\mathfrak{l}}$, $\alpha(f; \mathfrak{l})$ as before. This follows from the proof in [23, p. 5], in our case the generating function $\mathcal{F}(s)$ of $\pi_{\mathrm{sf},UN}(\mathfrak{g}) := \{n \text{ square-free }, (n, UN\ell) = 1, a(\mathfrak{g}, n) \not\equiv 0 \bmod \mathfrak{l}\}$ is just $\mathcal{F}(s) = \sum_{n\in\pi_{\mathrm{sf},UN}(\mathfrak{g})} n^{-s} = \prod_{p\in\pi_{\mathrm{sf},UN\ell}(\mathfrak{g})}(1 + p^{-s})$ and the subsequent arguments in [23] hold verbatim, leading to the asymptotic formula (3.33).

These take care of the lower bound for $\pi_{\mathrm{sf}}(f, x; \mathfrak{l})$. The argument for the upper bound remains the same as before. □

Example 3.12. We work out an explicit set of primes P outside of which one has an asymptotic formula for $\pi(\Delta^2, x)$ which conforms to Proposition 3.10. We refer the reader to the LMFDB database for some of our calculations here. Namely $\dim S_{24}(1) = 2$, and is spanned by two newforms say X_1 and X_2 written as

$$X_1(\tau) = q + (540 - \beta)q^2 + \cdots, \quad X_2(\tau) = q + (540 + \beta)q^2 + \cdots;$$

which are conjugate under the Galois group $G \simeq \mathbf{Z}/2\mathbf{Z}$ of the coefficient field $L = \mathbf{Q}(X_1) = \mathbf{Q}(X_2) = Q(\sqrt{D})$ where the fundamental discriminant D equals 144169. The Sturm's bound here is $\mathcal{S}^1(24, 1) = 2$ and the smallest prime q such that $a(X_1, q) \neq a(X_2, q)$ is $q = 2$. Following LMFDB, we put $\beta = 12\sqrt{D}$. Finally note that L has class number one, and that D is a prime number.

We let $\mathfrak{l} \subset O_L$ lie over ℓ. One easily checks that (again by using Sturm's bound)

$$\Delta^2 = \frac{-1}{2\beta} X_1 + \frac{1}{2\beta} X_2. \tag{3.34}$$

Hence if we request that

$$\mathfrak{l} \nmid 2\beta = 24\sqrt{D} \iff \ell \nmid 2 \cdot 3 \cdot D,$$

we would be able to write over $\mathfrak{l}$-integral numbers

$$\Delta^2 \equiv \frac{-1}{2\beta} X_1 + \frac{1}{2\beta} X_2 \bmod \mathfrak{l}. \tag{3.35}$$

This is all we need (of course here we got it much more directly, without using any analytic means like the Hecke bound) to obtain, by considering $T_2(\Delta^2) - a(X_2, 2)\Delta^2$ that

$$a(X_1, n) \equiv a(\Delta^2, 2n) - a(\Delta^2, n/2) - a(X_2, 2)a(\Delta^2, n) \bmod \mathfrak{l}.$$

Then considering n such that $(n, 6D\ell) = 1$, we find that

$$a(X_1, n) \equiv a(\Delta^2, 2n) - (540 + \beta)a(\Delta^2, n) \bmod \mathfrak{l},$$

which shows by a simple counting that

$$\pi(X_1, x; \mathfrak{l}) \leq \pi(\Delta^2, 2x; \mathfrak{l}). \tag{3.36}$$

Moreover (3.35) immediately implies (since X_1, X_2 are Galois conjugate) for any $j = 1, 2$,

$$\pi(\Delta^2, x; \mathfrak{l}) \leq \pi(X_j, x; \mathfrak{l}). \tag{3.37}$$

Combining (3.36) and (3.37), we see that for $x \geq 2$ and $\ell \nmid 6 \cdot 144169$

$$\pi(X_1, x/2; \mathfrak{l}) \leq \pi(\Delta^2, x; \mathfrak{l}) \leq \pi(X_j, x; \mathfrak{l}),$$

and by Serre [23] there is a constant $c(X_1, \ell)$ such that for any $\epsilon > 0$ and x large enough

$$\begin{aligned}\frac{1}{2}(1-\epsilon)c'(X_1, \ell)\frac{x}{(\log x)^{\alpha(X_1)}} &\leq \pi(\Delta^2, x; \mathfrak{l}) \\ &\leq (1+\epsilon)c(X_1, \ell)\frac{x}{(\log x)^{\alpha(X_1)}},\end{aligned} \tag{3.38}$$

for some positive quantities $c(X_1, \ell), c'(X_1, \ell)$ not depending on x. This is in contrast to the result in [5, 7.1.1] where $\ell = 3$ and an additional factor of $\log\log x$ was obtained in (3.38).

3.3.1. The quantity $h(f; \mathfrak{l})$ We now turn our attention to the quantity $h(f; \mathfrak{l})$, which is the exponent of $\log\log x$ appearing in (1.5).

Proposition 3.13. *Let k, N be fixed and $\mathfrak{l}$ be a prime in K lying over an odd prime ℓ. Suppose that for some $f \in M_k(\Gamma_1(N))(\mathcal{O}_K)$ which is not constant* mod $\mathfrak{l}$, *one has $h(f; \mathfrak{l}) \neq 0$. Then the following statements hold.*

(i) $\mathfrak{l} \mid \mathcal{L}(\{q_{i,j}\}; f)$ *for any set of primes $\{q_{i,j}\}$ admissible for f.*
(ii) *Suppose in addition that $f \in M_k(N, \chi)$ for some Dirichlet character χ* mod N. *There exists a pair $i, j \in S_f$ $(i \neq j)$ such that the congruences $b_i(n) \equiv b_j(n)$* mod $\mathfrak{l}$ *hold for all $n \geq 1$ with $(n, N) = 1$.*

Remark 3.14. In particular, (i) says that the quantity $h(f; \mathfrak{l})$ in (1.5) is 0 for all but finitely many ℓ. Moreover, choosing the admissible set to be $\{m_{i,j}\}$ from the introduction, and the bounds on $m_{i,j}$ from section 3.1.2, we see that $h(f; \mathfrak{l}) = 0$ for all $\ell > \mathcal{C}$, where $\mathcal{C}$ depends only on k and N.

Proof. Let f be as in the proposition and $\{q_{i,j}\}$ be admissible for f. If $\mathfrak{l} \nmid \mathcal{L}(\{q_{i,j}\}; f)$ then the sieving procedure described in the proof of Proposition 3.4 works, and then Proposition 3.10 shows that $h(f; \mathfrak{l}) = 0$. This proves (i).

For (ii), suppose that for all pairs $u \neq v$ $(u, v \in S_f)$ one has $b_u(n) \not\equiv b_v(n) \bmod \mathfrak{l}$ for some $(n, N) = 1$. Multiplicativity of the Fourier coefficients and Hecke relations imply that for each such pair $u \neq v$ there must be a prime, say $\mathbf{q}_{u,v}$ with $(\mathbf{q}_{u,v}, N) = 1$ such that $b_u(\mathbf{q}_{u,v}) \not\equiv b_v(\mathbf{q}_{u,v}) \bmod \mathfrak{l}$. Indeed this follows from the relation

$$b_t(p^j) = b_t(p)b_t(p^{j-1}) - p^{k-1}\chi(p)b_t(p^{j-2}) \qquad (j \geq 2, p \nmid N),$$

which shows that if $b_u(p) = b_v(p)$ on a set of primes $\mathfrak{P}$, then $b_u(n) = b_v(n)$ for all n away from $\mathfrak{P}$. That f_u, f_v have the same nebentypus is crucial here.

Then clearly $\{\mathbf{q}_{u,v}\}$ is an admissible set for f, and thus by the quantitative result from Proposition 3.10 we must have $h(f; \mathfrak{l}) = 0$. This contradiction finishes the proof of (ii). □

We record here another feature of the quantity $h(f; \mathfrak{l})$, whose proof is omitted since it is verbatim similar to that of Proposition 3.10. Let $\widetilde{M}(N)$ be the $\mathcal{O}_K/\mathfrak{l}$-vector space consisting of the reduction mod $\mathfrak{l}$ of elements of the algebra $\bigoplus_k M_k(\Gamma_1(N))(\mathcal{O}_K)$. Recall from [14] that a set $\{\lambda(p)\}_{(p,N)=1}$ is called a system of eigenvalues mod $\mathfrak{l}$ if there is an eigenform $g \in \widetilde{M}(N)$ such that $T(p)g = \lambda(p)g$ for all p.

Proposition 3.15. *Let ℓ be an odd prime and $\mathfrak{l}|\ell$. Let $f \in \widetilde{M}(N)$ be non-constant* mod $\mathfrak{l}$. *Suppose that f can be written as a finite linear combination of eigenforms (of all Hecke operators)* mod $\mathfrak{l}$ *whose system of eigenvalues are pairwise distinct. Then $h(f; \mathfrak{l}) = 0$.*

This leads us to formulate the following conjecture.

Conjecture 3.16. Let ℓ be an odd prime and $\mathfrak{l}|\ell$. Let $f \in \widetilde{M}(N)$ be non-constant mod $\mathfrak{l}$. Then $h(f; \mathfrak{l}) = 0$ if and only if f can be written as a finite linear combination of eigenforms (of all Hecke operators) mod $\mathfrak{l}$ whose system of eigenvalues are pairwise distinct.

The conjecture, if true, implies via Jochnowitz's result [14] on finitely many systems of eigenvalues mod ℓ that there are only finitely many $f \in \widetilde{M}(N)$ with $h(f; \mathfrak{l}) = 0$.

4. Siegel modular forms

First we discuss a Sturm bound for Siegel modular forms with level. This would be required to quantify the congruence primes in our results to follow. For the Sturm bound, we follow some arguments by Ram Murty [18]. For $T \in \Lambda_n^+$ we put

$$\mathcal{M}(T) := \max\{t_{1,1}, \ldots, t_{n,n}\}. \tag{4.1}$$

Proposition 4.1. *Let $F \in M_k^n(\Gamma_1(N))(\mathcal{O}_K)$ be such that $F \not\equiv 0 \bmod \mathfrak{l}$. Then there exist $T \in \Lambda_n$ with*

$$\mathcal{M}(T) \leq \left(\frac{4}{3}\right)^n \frac{k}{16}[\mathrm{Sp}(n, \mathbf{Z})\colon \Gamma_1(N)] =: \mathcal{S}^n(k, N) \tag{4.2}$$

such that $a_F(T) \not\equiv 0 \bmod \mathfrak{l}$.

Proof. The proof is analogous to the argument used in [18] (essentially by reducing to the case of level one as in [19] by using the 'norm' map) and we do not repeat it. We just note that the main two ingredients that go into the proof in [18], namely:

(i) $M_k^n(\Gamma_1(N))$ has a basis consisting of elements with Fourier coefficients in $\mathbf{Z}$;
(ii) if $F \in M_k^n(\Gamma_1(N))(\mathcal{O}_K)$, then in each cusp, it's Fourier coefficients are also in a number field and have bounded denominators;

are available from the work of Shimura [24]. □

Next we recall the notion of a singular Siegel modular form of degree n. Namely, F as Proposition 4.1 is called singular mod $\mathfrak{l}$ if $a_F(T) \equiv 0 \bmod \mathfrak{l}$ for all $T \in \Lambda_n^+$. We would not directly apply the following lemma in this paper, but would use it indirectly in order to provide a convenient hypothesis in Theorem 4.9. Also we believe this is not written down in the literature, and could be useful elsewhere.

Lemma 4.2. *Assume that N is coprime to ℓ (ℓ odd), $F \in M_k^n(\Gamma_1(N))(\mathcal{O}_K)$ and let $\mathfrak{l}$ be a prime of K dividing ℓ. Assume that F is $\mathfrak{l}$ singular of rank t, i.e.*

$$t = \max\{\mathrm{rank}(T) \mid T \in \Lambda_n,\ a_F(T) \not\equiv 0 \bmod \mathfrak{l}\}$$

with $1 \leq t \leq n-1$. Then $2k - t$ is divisible by $\ell - 1$.

This is just a $\Gamma_1(N)$ variant of Corollary 3.7 in [8] so we only give a brief sketch of proof.

Proof. The basic strategy is to associate with F an elliptic modular form g such that g is congruent mod $\mathfrak{l}$ to a unit in $\mathcal{O}_{\mathfrak{l}}$. We would see that g would be on $\Gamma_1(R)$ for some R such that R is coprime to p. The weight k' of such a modular form g must be divisible by $\ell - 1$ by Serre et al., and this would imply the same for the weight of F.

To do this, we may choose $T \in \Lambda_n$ of rank t with $a_F(T) \not\equiv 0 \bmod \mathfrak{l}$ to be of the form $T = \left(\begin{smallmatrix} 0 & 0 \\ 0 & T_0 \end{smallmatrix}\right)$ with $T_0 \in \Lambda_t^+$. Also, we may apply Siegel's Φ-operator several times to go to a modular form f of degree $t+1$. Then we consider the Fourier-Jacobi coefficient ϕ_{T_0} of f and its theta decomposition; the modular form h_0 in this theta decompositon is then congruent to a constant (unit) mod $\mathfrak{l}$. Furthermore h_0^2 is a modular form for $\Gamma_1(N) \cap \Gamma_0(M)$ with nebentypus character $\left(\frac{-4}{*}\right)$ where M is the level of $2T_0$; the weight is $2k - t$. If M is coprime to ℓ we may take $g := h_0^2$ and apply the statement from above. Otherwise, we write $M = \ell^s \cdot M'$ with M' coprime to ℓ and by standard level changing, there is a modular form g for $\Gamma_1(NM')$ of weight $2k - t + m \cdot (\ell - 1)$ for some nonnegative integer m with $g \equiv h_0^2 \bmod \mathfrak{l}$; now we argue as before with this g. □

Let us recall now the following result due to Böcherer-Nagaoka, which was used to prove that congruences between Siegel modular forms imply congruences between their weights. For $F \in M_k^n(\Gamma_1(N))(\mathcal{O}_K)$ we put

$$\nu_{\mathfrak{l}}(F) := \min_{T \in \Lambda_n} \nu_{\mathfrak{l}}(a_F(T)).$$

Proposition 4.3. ([9]) *Let $\mathfrak{l} \subset \mathcal{O}_K$ be a prime ideal. For every $F \in M_k^n(\Gamma_1(N))(\mathcal{O}_K)$ there exists for all sufficiently large $R \in \mathbf{N}$ an elliptic modular form $f \in M_k(\Gamma_1(NR^2))(\mathcal{O}_K)$ such that the Fourier coefficients of f are finite sums of those of F; and $\nu_{\mathfrak{l}}(f) = \nu_{\mathfrak{l}}(F)$.*

For future use, let us briefly recall the setting of the proof of the above proposition, in a slightly more general situation than that in [9]. Let $\mathcal{P}$ be a certain property satisfied by some of the Fourier coefficients of F.

As in [9], we consider the set

$$\mathcal{T} = \{T \in \Lambda_n \mid a_F(T) \text{ satisfies } \mathcal{P}\}.$$

We let d to be the minimum of the quantities $\mathcal{M}(T)$ (as defined in (4.1)) for $T \in \mathcal{T}$. Then we fix any $T_0 \in \mathcal{T}$ with $\mathcal{M}(T_0) = d$ and put $diag(T_0) = (d_1, \ldots, d_n)$.

We now consider the finite set

$$\mathcal{T}_d = \{T \in \mathcal{T} | \mathcal{M}(T) = d\}. \tag{4.3}$$

We next choose $R \geq 1$ 'large enough' (possibly with suitable additional conditions) such that $\{T \in \mathcal{T}_d | T \equiv T_0 \bmod R\} = \{T_0\}$.

We then put, borrowing the notation from [9]

$$F^{(R,T_0)}(Z) := \sum_{T \equiv T_0 \bmod R} a_F(T) e(TZ), \tag{4.4}$$

and define

$$f(\tau) = \sum_{r=0}^{\infty} a(f, r) q^r \in M_k(\Gamma_1(NR^2)) \tag{4.5}$$

by

$$a(f, r) = \sum_{T \equiv T_0 \bmod R,\, diag(T) = (r, d_2, \ldots, d_n)} a_F(T); \tag{4.6}$$

then one has

$$a(f, d_1) = a_F(T_0). \tag{4.7}$$

We now show that an adaptation of this technique to our setting can be used to show that any F is not constant mod $\mathfrak{l}$ as above has infinitely many $\mathrm{GL}(n, \mathbf{Z})$-inequivalent 'primitive' Fourier coefficients which are non-zero mod $\mathfrak{l}$ when ℓ is large enough. This generalises previous results on this topic by Zagier [28], Yamana [27] where the Fourier coefficients were in $\mathbf{C}$.

We need a bit of more notation. For $T \in \Lambda_n$ $(n \geq 2)$, let $\mathcal{D}(T)$ denote the greatest common divisor of all the diagonal elements of T except the first:

$$\mathcal{D}(T) = \gcd(t_{2,2}, \ldots, t_{n,n}). \tag{4.8}$$

Note that $\mathcal{D}(T) \in \mathbf{N}$ and that if $c(T)$ denotes the content of T, then $c(T) \mid \mathcal{D}(T)$.

Theorem 4.4. *Let F, which is not constant* mod $\mathfrak{l}$ *be as in Proposition 4.3. Suppose there exist $T \in \Lambda_n$ such that $a_F(T) \not\equiv 0 \bmod \mathfrak{l}$ with $(\mathcal{D}(T), N) = 1$. Then there exist infinitely many* $\mathrm{GL}(n, \mathbf{Z})$*-inequivalent primitive matrices $T \in \Lambda_n$ such that $a_F(T) \not\equiv 0 \bmod \mathfrak{l}$ for all ℓ (lying under $\mathfrak{l}$) effectively large enough in terms of only k, N; and in particular we request that $\ell > k + 1$.*

Proof. We will freely refer to the discussion preceeding this theorem. Here the property $\mathcal{P}$ is that $a_F(T) \not\equiv 0 \bmod \mathfrak{l}$ and $(\mathcal{D}(T), N) = 1$. Fix a $T = \mathbf{T}$ with this property.

The next three paragraphs are meant to show how to effectively bound the integer R from (4.4) in our situation. This would then tell us how large our ℓ has to be.

With such a $\mathbf{T}$ chosen, we now claim the existence of $T_0 \in \Lambda_n$ with the properties: $a_F(T_0) \not\equiv 0 \bmod \mathfrak{l}$, $(\mathcal{D}(T_0), N) = 1$ and $\mathcal{M}(T_0) = \max_i\{d_i\} \leq \mathcal{S}^n(k, N^2)$, where $\mathcal{S}^n(k, N)$ denotes the Hecke-Sturm bound for $M_k^n(\Gamma_1(N))$. Here for simplicity we have put $diag(T_0) = (d_1, d_2, \ldots, d_n)$.

Suppose to the contrary. Taking $\mathbf{1}_N$ to be the trivial Dirichlet character mod N and $L = L^t \in M_n(\mathbf{Z})$ satisfying the conditions:

$$L_{i,j} \equiv 0 \bmod N \; (i \neq j), \; L_{1,1} \equiv 0 \bmod N, \; \sum_{j=2}^{n} L_{j,j} d_j = \gcd(d_2, \cdots, d_n) = \mathcal{D}(\mathbf{T});$$

we then consider the Fourier series

$$G(Z) = \sum_T \mathbf{1}_N(\mathrm{tr}(LT)) a_F(T) e(TZ). \tag{4.9}$$

From Andrianov [3] we know that $G \in M_k^n(\Gamma)$, which is contained in $M_k^n(\Gamma_1(N^2))$ in view of the inclusions $\Gamma_1(N^2) \subset \Gamma \subset \Gamma_1(N)$, with $\Gamma = \{\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_1(N) | C \equiv 0 \bmod N^2\}$. Further our hypothesis on F shows that $G \not\equiv 0 \bmod \mathfrak{l}$ (indeed $a_G(\mathbf{T}) \not\equiv 0 \bmod \mathfrak{l}$).

By using the Sturm bound for $\Gamma_1^n(N^2)$ we get the existence of T_0 as claimed above, because the Fourier expansion of G in (4.9) is supported only on those T for which $(\mathcal{D}(T), N) = 1$.

We work with this T_0 as per the set-up described following Proposition 4.3 and also assume (without loss) that $\mathcal{M}(T_0) = d$ is the minimum with respect to the property $\mathcal{P}$. We then consider $\mathcal{T}_d$ as in (4.3) and proceed to choose R suitably.

We require three properties of such an R: it should be effectively bounded in terms of k, N; should be coprime to $\mathcal{D}(T_0)$; and should be big enough so that

$$\{T \in \mathcal{T}_d | T \equiv T_0 \bmod R, (\mathcal{D}(T), N) = 1\} = \{T_0\}.$$

We note that the following choice $R = ([2\mathcal{H}(k, N^2)]+1)\cdot\mathcal{D}(T_0)+1$ is good. This will ensure that one of the diagonal congruences for $T \equiv T_0 \bmod R$ does not hold in view of the definition of $\mathcal{T}_d$; further this choice also ensures that $(R, \mathcal{D}(T_0)) = 1$.

Next, we consider the modular form $f \in M_k(\Gamma_1(NR^2))$ from (4.5) with Fourier expansion as in (4.6) obtained from our F. Recall that by construction $\nu_{\mathfrak{l}}(f) = 0$, and we consider the Fourier coefficients $a(f, r)$ of f. Since $\ell > k + 1$, f is not constant mod $\mathfrak{l}$. From (4.7) it follows that if $a(f, r) \not\equiv 0 \bmod \mathfrak{l}$, there must exist $T \equiv T_0 \bmod R$ with $a_F(T) \not\equiv 0 \bmod \mathfrak{l}$ such that $diag(T) = (r, d_2, ..., d_n)$. Since $(\mathcal{D}(T_0), NR^2) = 1$ by our construction, we can apply Theorem 3.7 with $Q := \mathcal{D}(T_0)$ (note that the level of f divides NR^2) to deduce that there must exist infinitely many r such that $a(f, r) \not\equiv 0 \bmod \mathfrak{l}$ such that $(r, \mathcal{D}(T_0)) = 1$.

The crucial point is that for all the Fourier coefficients $a_F(T)$ $(T \equiv T_0 \bmod R)$ of $F^{(R,T_0)}$, one infers from (4.6) that $\mathcal{D}(T) = \mathcal{D}(T_0)$ $(= (d_2, \ldots, d_n))$. Therefore we get the existence a sequence of infinitely many matrices T such that $a_F(T) \not\equiv 0 \bmod \mathfrak{l}$ with the property that their diagonal entries have gcd to be 1. This implies that the T under consideration are all primitive.

Unfortunately this *does not* imply that all the primitive T obtained in this way are inequivalent under the action of $\mathrm{GL}(n, \mathbf{Z})$. However if $T \in \Lambda_n^+$, we can directly invoke Proposition 4.6, whose statement and proof however are deferred until the end of this proof, to get hold of infinitely many such matrices which are pairwise distinct mod $\mathrm{GL}(n, \mathbf{Z})$. Otherwise if $\mathrm{rank}(T) = s < n$, we can find $U \in \mathrm{GL}(n, \mathbf{Z})$ such that $T[U] = \begin{pmatrix} \widetilde{T} & 0 \\ 0 & 0 \end{pmatrix}$. Then we can consider $G(Z) := \Phi^{n-s}(F)(Z) = \sum_{S\in\Lambda_s} a_F(\left(\begin{smallmatrix} S & 0 \\ 0 & 0 \end{smallmatrix}\right))e(SZ)$, $(Z \in \mathbf{H}_s)$. Clearly $G \not\equiv 0 \bmod \mathfrak{l}$ and in particular $a_G(\widetilde{T}) \not\equiv 0 \bmod \mathfrak{l}$ with $\widetilde{T} \in \Lambda_s^+$ primitive. Thus we can again invoke Proposition 4.6 to G to conclude the existence of infinitely many primitive $S \in \Lambda_s^+/\mathrm{GL}(s, \mathbf{Z})$ such that $a_G(S) \not\equiv 0 \bmod \mathfrak{l}$. To conclude the same result for F, note that the matrices $\left(\begin{smallmatrix} S & 0 \\ 0 & 0 \end{smallmatrix}\right)$ obtained above as also pairwise distinct mod $\mathrm{GL}(n, \mathbf{Z})$. This follows from the statement that $S_1, S_2 \in \Lambda_s^+$ are $\mathrm{GL}(s, \mathbf{Z})$ equivalent if and only if $\left(\begin{smallmatrix} S_1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} S_2 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ are $\mathrm{GL}(n, \mathbf{Z})$ equivalent. One side of the implication is trivial, to see the other; suppose that $U = \left(\begin{smallmatrix} U_1 & U_2 \\ U_3 & U_4 \end{smallmatrix}\right) \in \mathrm{GL}(n, \mathbf{Z})$ be such that

$$\begin{pmatrix} U_1^t & U_3^t \\ U_2^t & U_4^t \end{pmatrix} \begin{pmatrix} S_1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} U_1 & U_2 \\ U_3 & U_4 \end{pmatrix} = \begin{pmatrix} S_2 & 0 \\ 0 & 0 \end{pmatrix}.$$

A short calculation shows that $U_1^t S_1 U_1 = S_2$ and $U_2^t S_1 U_2 = 0$. The positive-definiteness of S_1 forces $U_2 = 0$ and thus $U_1 \in \mathrm{GL}(s, \mathbf{Z})$. Since the content is preserved under the action of $\mathrm{GL}(n, \mathbf{Z})$, we are therefore done.

While applying Theorem 3.7 we needed to ensure that ℓ is large enough only in terms of k, N, R. But since $\mathcal{D}(T_0)$, and hence R (see our choice of R) can be estimated (explicitly) as a polynomial in k, N; ℓ is large enough depending only on k, N. We do not work this out. □

It remains to prove Proposition 4.6. Let us recall the Fourier-Jacobi expansion of F of type $(1, n-1)$ from (2.8). Let ϕ_S be the Fourier-Jacobi coefficients. By tacitly identifying ϕ_S with the associated function $\varphi_S = \phi_S \cdot e(SZ)$ (cf. section 2), we refer to the Fourier coefficients of ϕ_S as supported on matrices of the form $\left(\begin{smallmatrix} * & * \\ * & S \end{smallmatrix}\right) \in \Lambda_n$. From (2.6) the Fourier expansion of the theta components h_μ of ϕ_S:

$$h_\mu(\tau) = \sum_r b(r, \mu) e\left((r - S^{-1}[\mu/2]) \cdot \tau\right). \tag{4.10}$$

Lemma 4.5. *With the above notation, suppose that for all $S \in \Lambda_{n-1}^+$ and all $\mu \in \mathbf{Z}^{n-1}/2S\mathbf{Z}^{n-1}$ we have $b(r, \mu) \not\equiv 0 \bmod \mathfrak{l}$ only for finitely many values of $r - S^{-1}[\mu]$ with r coprime to $\gamma(\mu)$, where $\gamma(\mu) := \gcd(\mu, c(S))$. Then the Fourier expansion of $\phi_S \bmod \mathfrak{l}$ is supported on matrices $T = \begin{pmatrix} r & \mu^t \\ \mu & S \end{pmatrix} \in \Lambda_n$, with* $\mathrm{rank}(T) \leq n-1$.

Proof. We start from the theta expansion (2.5) of ϕ_S. We observe that for a Fourier series as in (2.6) the invariance property (2.7) is equivalent to the possibility writing down a "theta expansion" as in (2.5). This observation will be used soon.

We put $b(r, \mu)^* := b(r, \mu)$ if the gcd of r, μ and of the content $c(S)$ is one and we define $b(r, \mu)^*$ to be zero otherwise. We observe that the gcd of r, μ and of $c(S)$ is the same as the gcd of $r + L^t \cdot \mu + S[L]$, $\mu + 2S \cdot L$ and of $c(S)$. This implies that the subseries of ϕ_S, defined by

$$\phi_S^*(\tau, z) = \sum_{r,\mu} b(r, \mu)^* e(r\tau + \mu^t z)$$

still has an expansion (keeping in mind the observation from the first paragraph)

$$\phi_S^*(\tau, z) = \sum_{\mu_0} h_{\mu_0}^*(\tau) \Theta_S[\mu_0](\tau, z)$$

where the $h_{\mu_0}^*$ are given by subseries of the Fourier expansion of h_{μ_0}, more precisely, we have

$$h_{\mu_0}^*(\tau) = \sum_r b(r, \mu_0)^* e\left((r - S^{-1}\left[\frac{\mu_0}{2}\right]) \cdot \tau\right).$$

For fixed μ_0 we may rephrase the condition defining $b(r, \mu_0)^*$ as saying that the gcd of r and $\gamma(\mu_0)$ is one where $\gamma(\mu) :=$ gcd of μ and of $c(S)$.

This can be rephrased in terms of the summation index $r - S^{-1}[\frac{\mu_0}{2}]$ by

$$r - S^{-1}\left[\frac{\mu_0}{2}\right] \notin -S^{-1}\left[\frac{\mu_0}{2}\right] + q \cdot \mathbf{Z}$$

for any prime q dividing $\gamma(\mu_0)$. In particular, $h_{\mu_0}^*$ is still a modular form of some level because it is extracted from the modular form h_{μ_0} by some coprimality condition for its summation index.

By hypothesis, for all μ_0 there are only finitely many $r - S^{-1}[\mu_0]$ with r coprime to $\gamma(\mu_0)$ such that $b(r, \mu_0) \not\equiv 0 \bmod \mathfrak{l}$. Then by [22] or Theorem 3.1 in [8] the $h^*_{\mu_0}$ are constant functions mod $\mathfrak{l}$:

$$\phi^*_S \equiv \sum b(r, \mu_0)\Theta_S[\mu_0](\tau, z) \bmod \mathfrak{l}$$

where r and μ_0 satisfy $r = S^{-1}[\frac{\mu_0}{2}]$ (see (4.10)) and $(r, \gamma(\mu_0)) = 1$. In particular, the Fourier expansion of ϕ^*_S mod $\mathfrak{l}$ is supported on matrices $T \in \Lambda_n$, with $\mathrm{rank}(T) \leq n - 1$. □

Proposition 4.6. *If $F \in M^n_k(\Gamma_1(N))$ is such that it is not constant* mod $\mathfrak{l}$*; then the set*

$$\{T \in \Lambda^+_n \mid T \textit{ primitive}\ , a_F(T) \not\equiv 0 \bmod \mathfrak{l}\}/\mathrm{GL}(n, \mathbf{Z})$$

is either empty or infinite.

Remark 4.7. The same statement, but without primitivity condition appears in [8].

Proof. We assume that the set in question is indeed non-empty and finite with $\{L_1, \ldots, L_t\}$ ($t \geq 1$) as a set of representatives. Let ϕ_S be the Fourier-Jacobi coefficients of F of type $(1, n-1)$. Then ϕ_S can carry a mod $\mathfrak{l}$ nonzero primitive Fourier coefficient only if $S = L_i[G]$ for some primitive $G \in \mathbf{Z}^{(n,n-1)}$. To see this, recall we have identified ϕ_S with φ_S. Suppose φ_S carries a Fourier coefficient at $\widetilde{S} \in \Lambda_n$. Necessarily $\widetilde{S} = L_i[U]$ for some $U \in \mathrm{GL}(n, \mathbf{Z})$:

$$\widetilde{S} = \begin{pmatrix} r & \mu_0 \\ \mu_0^t & S \end{pmatrix}, \quad \widetilde{S} = L_i[U] = \begin{pmatrix} * & * \\ * & L_i[G] \end{pmatrix}.$$

Furthermore, for fixed S we observe that $\det L_i = \det(S) \cdot (r - S^{-1}[\mu_0])$ and hence $r - S^{-1}[\mu_0]$ is from a finite set. Since L_i is primitive, necessarily $\gcd(r, \gamma(\mu_0)) = 1$, where recall that $\gamma(\mu_0) = \gcd(\mu_0^t, c(S))$. We may now apply Lemma 4.5 to see that the rank condition for the L_i cannot be satisfied. This contradiction finishes the proof. □

Remark 4.8. The reasoning above also works in the Archimedean setting.

4.1. Quantitative results: Siegel modular forms

In this subsection, we collect various quantitative results on the number of nonvanishing Fourier coefficients mod $\mathfrak{l}$ of Siegel modular forms, which essentially follow from the corresponding statements about elliptic modular forms. For $M \in \Lambda^+_n$ denote by d_M its 'absolute discriminant' (i.e., ignoring the usual sign), defined by

$$d_M := |\mathrm{disc.}(2M)| = \begin{cases} \det(2M) \text{ if } n \text{ is even,} \\ \\ \frac{1}{2}\det(2M) \text{ if } n \text{ is odd.} \end{cases} \tag{4.11}$$

Note that $d_M \in \mathbf{N}$. Let $F \in M_k^n(\Gamma_1(N))(\mathcal{O}_K)$ and define the sets (suppressing the dependence on $\mathfrak{l}$ for convenience, unless there is a danger of confusion):

$$\begin{aligned}\pi_F(x, \det) &:= \{d \le x | a_F(T) \not\equiv 0 \bmod \mathfrak{l} \text{ for some } T \in \Lambda_n^+ \text{ such that } d_T = d\},\\ \pi_F(x, \det; \mathrm{sf}) &:= \pi_F(x, \det) \cap \{\text{Odd square-free numbers}\},\\ \pi_F(x, \det; \mathrm{pr}) &:= \pi_F(x, \det) \cap \{\text{Odd prime numbers}\},\\ \pi_F(x, \mathrm{tr}) &:= \{d \le x | a_F(T) \not\equiv 0 \bmod \mathfrak{l} \text{ for some } T \in \Lambda_n^+ \text{ such that } \mathrm{tr}(T) = d\}.\end{aligned}$$

Theorem 4.9. *Let $F \in M_k^n(\Gamma_1(N))$ be non-singular* mod $\mathfrak{l}$*. Then for some $0 < \beta(F) \le 3/4$,*

$$(a1)\quad |\pi_F(x, \det)| \gg_F \frac{x}{(\log x)^{\beta(F)}} \quad (n \textit{ odd}),$$

$$(a2)\quad |\pi_F(x, \det)| \gg_F \frac{\sqrt{x}}{(\log\log x)} \quad (n \textit{ even}),$$

$$(b)\quad |\pi_F(x, \det; \mathrm{sf})| \gg \frac{x}{(\log x)^{\beta(F)}} \quad (n \textit{ odd}, N = 1, k \ge (n+3)/2, \ell \gg_F 1),$$

$$(c)\quad |\pi_F(x, \det; \mathrm{pr})| \gg \frac{x}{(\log x)} \quad (n \textit{ odd}, N = 1, k \ge (n+3)/2).$$

In view of Lemma 4.2, parts $(a1)$, $(a2)$, (c) the above theorem therefore hold for all ℓ such that $\ell - 1 \ge k - n$.

Proof. Since F is non-singular mod $\mathfrak{l}$, we first get hold of $T \in \Lambda_n^+$ such that $a_F(T) \not\equiv 0 \bmod \mathfrak{l}$, say for concreteness that $\det(T)$ is minimal with this property.

Let T_0 be the right lower diagonal block of T of size $n-1$. We look at the T_0-th Fourier-Jacobi coefficient, say ϕ, of F. We consider any of it's theta components, say h_μ ($\mu \in \mathbf{Z}^{n-1}/2T_0 \cdot \mathbf{Z}^{n-1}$), which is $\not\equiv 0 \bmod \mathfrak{l}$. Such a h_μ exists since $\phi \not\equiv 0 \bmod \mathfrak{l}$. It is well-known that $H(\tau) := h_\mu(4d_{T_0}\tau)$ is in $M_\kappa(\Gamma_1(M))$ with $M = 16d_{T_0}^2 N$ and $\kappa := k - (n-1)/2$. We note that the Fourier coefficients of H and F are related as (for this and the above facts, see e.g., [7, section 2.3]):

$$\begin{aligned} a(H, n) &= a_F(\begin{pmatrix} n/4d_{T_0} + T_0^{-1}[\mu/2] & \mu/2 \\ \mu^t/2 & T_0 \end{pmatrix}), \\ &(n/4d_{T_0} + T_0^{-1}[\mu/2] \in \mathbf{N}). \end{aligned} \tag{4.12}$$

We now have two avenues. Since T_0 is fixed, we can get (in an elementary way) $(a1)$ from (4.12) by applying Proposition 3.10 to H (which is non-constant mod $\mathfrak{l}$) and taking $\beta(F) := \alpha(H)$ if n is odd. However we use the stronger result in [5, Theorem 1] which holds for all ℓ. Since n is even in $(a2)$, we apply [6, Theorem 1] to H and are done.

For (b), by combining the main result Theorem 1.1 with Proposition 3.8 of [7] we choose $\mathbf{T} = \begin{pmatrix} \mathbf{n} & r/2 \\ r^t/2 & T_0 \end{pmatrix} \in \Lambda_n^+$ to be such that $a_F(\mathbf{T}) \ne 0$, d_{T_0} being odd, square-free and r is 'T_0-primitive', i.e., the denominator of $T_0^{-1}(r/4)$ is exactly d_{T_0}. We then choose a prime $\mathfrak{l} \subset O_K$ such that $\mathfrak{l} \nmid a_F(\mathbf{T})$ by requesting $\ell \gg_F 1$ to be large enough (here $\mathfrak{l} \mid \ell$), e.g., by using the Hecke's bound on Fourier coefficients of modular forms. We can additionally ensure that $d_{\mathbf{T}}$ is odd and square-free as well; this follows by combining the last assertion in Proposition 3.8 of [7] with Theorems 4.3 and 4.6 of [7] and of course can be read off from [7, Theorem 1.1].

Arguing as in the previous paragraph we now put $H(\tau) := h_\mu(d_{T_0}\tau)$ and note that H has level $\Gamma_1(d_{T_0}^2)$ such that H is not a constant mod $\mathfrak{l}$ and H is related to F by (4.12) where we replace $4d_{T_0}$ by d_{T_0}. Additionally we define $\widetilde{H}(\tau) = \sum_{(n,2)=1} a(H,n)q^n$. We can also write $\widetilde{H}$ as $\widetilde{H}(\tau) = \sum_{(n,2d_{T_0})=1} a(H,n)q^n$ since d_{T_0} is odd and $a(H,n) \neq 0$ only if $(n, d_{T_0}) = 1$. The latter assertion follows since r is 'T_0-primitive', see [7, subsection 3.4.1]. Then [7, Lemma 4.1] shows that $\widetilde{H} \neq 0$. This construction of $\widetilde{H}$ is required to assure the existence of *odd* and square-free integers n such that $a(H,n) \not\equiv 0 \bmod \mathfrak{l}$. This is so that we can consider 'fundamental' Fourier coefficients of F, which are our objects of interest, adjusting signs if necessary.

We note that $a(\widetilde{H}, \widetilde{\mathbf{n}}) \not\equiv 0 \bmod \mathfrak{l}$ for some square-free $\widetilde{\mathbf{n}}$. For example we can choose $\widetilde{\mathbf{n}} := d_{T_0}(\mathbf{n} - T_0^{-1}[r/4])$, simply because $\widetilde{\mathbf{n}} = d_{\mathbf{T}}$ and $d_{\mathbf{T}}$ is odd and square-free. See [7, subsection 3.4.1]. Therefore we are done by applying the first part of [5, Theorem 26] to $\widetilde{H}$. The lower bound in (b) then follows from that of $\widetilde{H}$, upon using (4.12).

Finally arguing exactly as in the proof of (b) above, but this time using [7, section 5, Theorem 5.1], (c) follows from [4, Thm. I]. This completes the proof. □

Remark 4.10. It is possible to prove (b) by not invoking the full force of the main result (Theorem 1.1) from [7] but only by using the weaker hypothesis that F has a Fourier-Jacobi coefficient ϕ_{T_0} of index $T_0 \in \Lambda_{n-1}^+$ such that ϕ_{T_0} is not a constant mod $\mathfrak{l}$ and d_{T_0} is odd and square-free. This amounts to not assuming that $d_{\mathbf{T}}$ in the above proof is odd and square-free to begin with. For completeness we include a proof, which is as follows.

Keeping the above notation and assumption, we look at $\widetilde{H}$. We claim that $\widetilde{H}$ is not a constant mod $\mathfrak{l}$. Otherwise $a(H,n) \equiv 0 \bmod \mathfrak{l}$ for all n such that $(n,2) = 1$ and this implies that H is a constant mod $\mathfrak{l}$ upon using Corollary 3.9. Next recall from [7], $a(H,n) \neq 0$ only if $(n, d_{T_0}) = 1$. This is because r, as in the above proof, is 'T_0-primitive'. If there exists a square-free n such that $a(\widetilde{H}, n) \not\equiv 0 \bmod \mathfrak{l}$, then we are done. Otherwise from the condition in (the second half of) [5, Theorem 26], we conclude that $a(\widetilde{H}, n) \not\equiv 0 \bmod \mathfrak{l}$ only for those n which are divisible by ν^2 with $\nu \mid 4d_{T_0}\ell$ for some prime ν (recall that the level of $\widetilde{H}$ divides $4d_{T_0}$). If $a(H, \nu^2 m) \not\equiv 0 \bmod \mathfrak{l}$ is such a Fourier coefficient, it must be true that $\nu \nmid d_{T_0}$. Otherwise there will exist a Fourier coefficient $a(H, \nu^2 m) \not\equiv 0 \bmod \mathfrak{l}$ in the Fourier expansion of H such that $(\nu^2 m, d_{T_0}) > 1$, contradicting the support of the set $a(H,n) \bmod \mathfrak{l}$ as n varies.

Thus $\nu = 2$ or ℓ and in any case we see that $(2\ell, d_{T_0}) = 1$. Therefore from Theorem 3.7 (a) (again using that ℓ is large enough so as to satisfy the hypothesis of Theorem 3.7) we would then have a contradiction unless $\widetilde{H}$ is a constant mod $\mathfrak{l}$. The lower bounds would then follow from H as before.

Remark 4.11. It is not clear whether the arguments of [6] can be adapted to deal with square-free Fourier coefficients. In this regard, the method of this paper also does not work for half-integral weight modular forms, since the Hecke operators there are indexed by squares. If one had such a result, then part (b) above would have a version for even n as well.

Remark 4.12. The lower bound on ℓ in (b) can be made more explicit if we know bounds on the smallest d_T (say of the form $d_T \ll k^{a_n} N^{b_n}$) for the fundamental T such that $a_F(T) \neq 0$ *for all* n. This seems known only for $n = 1$ from [2].

Remark 4.13. In light of Theorem 4.9 (b), it may seem that Theorem 4.4 is redundant; but the former is only for odd n, whereas the latter is for all n. Moreover the lower bound on ℓ in Theorem 4.4 is effective only in terms of the weight and level of the concerned space, whereas in the case of Theorem 4.9 (b), it is dependent on the modular form.

We end by noting a nonvanishing result in terms of the trace function.

Proposition 4.14. *Let $F \in M_k^n(\Gamma_1(N))$ such that F is not constant* $\bmod \mathfrak{l}$. *Then for all primes* $\mathfrak{l}$,

$$|\pi_F(x, \mathrm{tr})| \gg \frac{x}{(\log x)^{\beta(F)}}. \tag{4.13}$$

Proof. We apply the procedure discussed after Theorem 4.4 to F. Here the property $\mathcal{P}$ is that $a_F(T) \not\equiv 0 \bmod \mathfrak{l}$. The proof then follows trivially from (4.6), (4.7) and [5, Thm. 1]. If one wishes to settle for more simple minded proof, then Proposition 3.10 may be used, but at the price of ℓ being large. In any case we put $\beta(F) := \alpha(f)$, where f is as given in (4.5). □

Acknowledgements S.D. was supported by a Humboldt Fellowship from the Alexander von Humboldt Foundation at Universität Mannheim during the preparation of the paper, and thanks both for the generous support and for providing excellent working conditions. The authors acknowledge the use of the LMFDB databse for some numerical computations. S.D also thanks IISc. Bangalore, DST (India) and UGC-CAS for financial support. During the preparation of this work S.D. was supported by a MATRICS grant MTR/2017/000496 from DST-SERB, India. We thank M. Raum for his comments on Siegel modular forms mod p. We are thankful to the referee for a thorough checking of the paper and for giving valuable suggestions which improved the content.

References

[1] Anamby, P., Das, S.: Distinguishing Hermitian cusp forms of degree 2 by a certain subset of all Fourier coefficients. Publ. Mat. **63**(1), 307–341 (2019)
[2] Anamby, P., Das, S.: Hecke-Siegel type threshold for square-free Fourier coefficients: an improvement. In: RIMS Kokyuroku Kyoto Univ., Proceedings for the Conference "Analytic and Arithmetic Theory of Automorphic Forms" (2018)
[3] Andrianov, A.N.: Twisting of Siegel modular forms with characters, and L-functions 1012 (Russian. Russian summary). Algebra i Analiz **20**(6), 1–29 (2008), translation in St: Petersburg Math. J. **20**(6), 851–871 (2009)

[4] Balog, A., Ono, K.: The Chebotarev density theorem in short intervals and some questions of Serre. J. Number Theory. **91**(2), 356–371 (2001)

[5] Bellaïche, J.: Image of pseudo-representations and coefficients of modular forms modulo p. Adv. Math. **353**, 647–721 (2019)

[6] Bellaïche, J., Soundararajan, K.: The number of nonzero coefficients of modular forms (mod p). Algebra Number Theory **9**(8), 1825–1856 (2015)

[7] Bellaïche, J., Green, B., Soundararajan, K.: Nonzero coefficients of half-integral weight modular forms mod ℓ. Res. Math. Sci. **5**(1), 10 (2018)

[8] Böcherer, S., Das, S.: On fundamental Fourier coefficients of Siegel modular forms. https://sites.google.com/site/somuhomepage/. https://arxiv.org/abs/1810.00762

[9] Böcherer, S., Kikuta, T.: On mod p singular modular forms. Forum Math. **28**(6), 1051–1065 (2016)

[10] Böcherer, S., Nagaoka, S.: Congruences for Siegel modular forms and their weights. Abh. Math. Semin. Univ. Hambg. **80**(2), 227–231 (2010)

[11] Das, S.: Omega results for Fourier coefficients of half-integral weight and Siegel modular forms. In: Springer Proceedings of Mathematics and Statistics, Procedding of the Conference at KSoM, Kerala in Honour of Prof. M. Manickam's 60th Birthday

[12] Hida, H.: On congruence divisors of cusp forms as factors of the special values of their zeta functions. Invent. Math. **64**(2), 221–262 (1981)

[13] Hida, H.: Congruence of cusp forms and special values of their zeta functions. Invent. Math. **63**(2), 225–261 (1981)

[14] Iwaniec, H., Kowalski, E.: Analytic Number Theory, Am. Math. Soc, vol. 53. Colloquium Publications (2004)

[15] Jochnowitz, N.: Congruences between systems of eigenvalues of modular forms. Trans. Am. Math. Soc. **270**(1), 269–285 (1982)

[16] Kohnen, W.: On Fourier coefficients of modular forms of different weights. Acta Arith. **113**(1), 57–67 (2004)

[17] Lichtenstein, S.: The effective Chebotarev density theorem and modular forms modulo $\mathfrak{m}$. Proc. Am. Math. Soc. **136**(10), 3419–3428 (2008)

[18] Miyake, T.: Modular forms. Translated from the 1976 Japanese original by Yoshitaka Maeda. Reprint of the first 1989 English edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, x+335 pp (2006)

[19] Ram Murty, M.: Bounds for congruence primes. In: Automorphic Forms, Automorphic Representations, and Arithmetic (Fort Worth, TX, 1996), Proceedings of Symposium Pure Mathematics, vol. 66, Part 1, Amer. Math. Soc., Providence, RI, pp. 177–192 (1999)

[20] Raum, M., Richter, O.K.: Sturm bounds for Siegel modular forms. Res. Number Theory **1**, 8 (2015)

[21] Ribet, K.: Mod p Hecke operators and congruences between modular forms. Invent. Math. **71**(1), 193–205 (1983)

[22] Saha, A.: Siegel cusp forms of degree 2 are determined by their fundamental Fourier coefficients. Math. Ann. **355**(1), 363–380 (2013)

[23] Serre, J.P.: Formes modulaires et fonctions zeta p-adiques. In: Modular Functions of One Variable III, Lecture Notes in Mathematics, vol. 350, Springer Verlag, pp. 191–268 (1973)

[24] Serre, J.P.: Divisibilité de certaines fonctions arithmétiques. Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 16, no°1, exp. no° 20, pp. 1–28 (1974–1975)

[25] Shimura, G.: On the Fourier coefficients of modular forms of several variables. Nachr. Akad. Wiss. Göttingen Math. Phys. Kl., vol. II, no. 17, pp. 261–268 (1975)

[26] Ventosa, X.T.: Theoretical and algorithmic aspects of congruences between modular Galois representations. PhD Thesis, Dissertation zur Erlangung des Grades eines Doktors der Naturwissenschaften Dem Fachbereich 6 (Mathematik und Informatik) der Universität Duisburg-Essen, 14 April (2009)
[27] Weisinger, J.: Some results on classical Eisenstein series and modular forms over function fields. Harvard Univ, Thesis (1977)
[28] Yamana, S.: Determination of holomorphic modular forms by primitive Fourier coefficients. Math. Ann. **344**, 853–863 (2009)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.