

Algebra & Number Theory

Volume 9

2015

No. 8

**The number of nonzero coefficients
of modular forms (mod p)**

Joël Bellaïche and Kannan Soundararajan



The number of nonzero coefficients of modular forms (mod p)

Joël Bellaïche and Kannan Soundararajan

Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a modular form modulo a prime p , and let $\pi(f, x)$ be the number of nonzero coefficients a_n for $n < x$. We give an asymptotic formula for $\pi(f, x)$; namely, if f is not constant, then

$$\pi(f, x) \sim c(f) \frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f)},$$

where $\alpha(f)$ is a rational number such that $0 < \alpha(f) \leq 3/4$, $h(f)$ is a nonnegative integer and $c(f)$ is a positive real number. We also discuss the equidistribution of the nonzero values of the coefficients a_n .

1. Introduction

Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a holomorphic modular form of integral weight $k \geq 0$ and some level $\Gamma_1(N)$ such that the coefficients a_n are integers. Let p be a prime number. Serre [1976] has shown that the sequence $a_n \pmod{p}$ is *lacunary*. That is, the natural density of the set of integers n such that $p \nmid a_n$ is 0. More precisely, Serre gave the asymptotic upper bound

$$|\{n < x, a_n \not\equiv 0 \pmod{p}\}| \ll \frac{x}{(\log x)^\beta}, \quad (1)$$

where β is a positive constant depending on f . Later, Ahlgren [1999, Lemma 2.1] established the following asymptotic lower bound: assume that p is odd and that there exists an integer $n \geq 2$ divisible by at least one prime ℓ not dividing Np such that $p \nmid a_n$. Then

$$|\{n < x, a_n \not\equiv 0 \pmod{p}\}| \gg \frac{x}{(\log x)}. \quad (2)$$

Joël Bellaïche was supported by NSF grant DMS 1101615. Kannan Soundararajan was partially supported by NSF grant DMS 1001068 and a Simons Investigator grant from the Simons Foundation. *MSC2010*: primary 11F33; secondary 11F25, 11N25, 11N37.

Keywords: modular forms modulo p , Hecke operators, Selberg–Delange’s method.

Under the same hypothesis, this lower bound was recently improved by Chen [2012]: for every $K \geq 0$,

$$|\{n < x, a_n \not\equiv 0 \pmod{p}\}| \gg \frac{x}{(\log x)} (\log \log x)^K, \tag{3}$$

where the implicit constant depends on K .

We improve on results (1), (2) and (3) by giving an asymptotic formula for $|\{n < x, a_n \not\equiv 0 \pmod{p}\}|$. To describe our results, we slightly change our setting by working directly with modular forms over a finite field, which allows for more generality and more flexibility.

Let p be an odd prime¹ and $N \geq 1$ an integer. We define the space of modular forms of level $\Gamma_1(N)$ with coefficients in \mathbb{F}_p , denoted by $M(N, \mathbb{F}_p)$, as the subspace of $\mathbb{F}_p[[q]]$ generated by the reductions modulo p of the q -expansions at ∞ of all holomorphic modular forms of level $\Gamma_1(N)$ and some integral weight $k \geq 0$ with coefficients in \mathbb{Z} . For \mathbb{F} a finite extension of \mathbb{F}_p , we define $M(N, \mathbb{F})$ as $M(N, \mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}$. Given f in $M(N, \mathbb{F})$, let

$$\pi(f, x) = |\{n < x : a_n \neq 0\}|.$$

Theorem 1. *Let $f = \sum_{n=0}^{\infty} a_n q^n \in M(N, \mathbb{F})$, and assume that f is not constant; that is, assume $a_n \neq 0$ for some $n \geq 1$. Then there exists a rational number $\alpha(f)$ with $0 < \alpha(f) \leq 3/4$, an integer $h(f) \geq 0$, and a positive real constant $c(f) > 0$ such that*

$$\pi(f, x) \sim c(f) \frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f)}.$$

This theorem was established by Serre [1976] for the case when f is an *eigenform* for all Hecke operators T_m (that is, $T_m f = \lambda_m f$, $\lambda_m \in \mathbb{F}$), and in this case one has $h(f) = 0$. However, the case of eigenforms is special because, as shown by Atkin, Serre, Tate and Jochnowitz in the 1970s, there are only finitely many normalized eigenforms in the infinite-dimensional space $M(N, \mathbb{F})$. One can decompose every $f \in M(N, \mathbb{F})$ as a finite sum $\sum_i f_i$ of *generalized eigenforms*² f_i but this fact does not seem to be of immediate use, for two reasons. The methods for treating genuine eigenforms do not seem to apply readily to generalized eigenforms, and moreover it is not clear how to obtain an asymptotic formula for $\pi(f, x)$ from asymptotics for $\pi(f_i, x)$. For f an eigenform, the main tool in Serre’s study is the Galois representation over a finite field attached to f by Deligne’s construction, $\bar{\rho}_f : G_{\mathbb{Q}, Np} \rightarrow \text{GL}_2(\mathbb{F})$. To deal with a general modular form f we replace ρ_f by a two-dimensional Galois *pseudorepresentation*, t_f ,

¹When $p = 2$, similar but slightly different results may be obtained, see [Bellaïche and Nicolas 2015].

²We call a form $f \in M(N, \mathbb{F})$ a *generalized eigenform* if, for every ℓ not dividing Np , there exist $\lambda_\ell \in \mathbb{F}$ and $n_\ell \in \mathbb{N}$ such that $(T_\ell - \lambda_\ell)^{n_\ell} f = 0$.

of $G_{\mathbb{Q}, Np}$ over a *finite ring* A_f . The ring A_f is obtained as the quotient of A by the annihilator of f , where A is the Hecke algebra acting on the space of modular forms $M(N, \mathbb{F})$. The ring A_f is not in general a field. In fact, it is a field precisely when f is an eigenform for the Hecke operators T_ℓ ($\ell \nmid Np$). The Hecke algebra A (at least in the case of $\Gamma_0(N)$) was introduced and studied in the wake of Swinnerton-Dyer’s work on congruences between modular forms by Serre, Tate, Mazur, Jochnowitz and others. More recent progress on understanding its structure may be found in [Nicolas and Serre 2012a; 2012b; Bellaïche and Khare 2015]. In Section 3, we recall the definitions of the Hecke algebra A , its quotient A_f , and the pseudorepresentation t_f and gather the results we need pertaining to them.

To prove Theorem 1, we introduce the notion of a *pure form*. A form f is *pure* if every Hecke operator T_ℓ (with $\ell \nmid Np$) in A_f is either invertible or nilpotent. Generalized eigenforms are pure since the finite ring A_f is local in this case, but there are pure forms that are not generalized eigenforms. For pure forms we can give a reasonable description of the set of integers n with $(n, Np) = 1$ and such that $a_n \neq 0$, and using this and a refinement of the Selberg–Delange method (see Section 2) we deduce (in Section 4A) an asymptotic formula for the number of $n \leq x$ with $a_n \neq 0$ and $(n, Np) = 1$. For a general f , we show in Section 4B that if $f = \sum_i f_i$ is a minimal decomposition of f into pure forms, then $\pi(f, x)$ is asymptotically $\sum_i \pi(f_i, x)$. To complete the proof of Theorem 1, it remains to handle coefficients a_n with $(n, Np) > 1$, and this is treated in Section 4C.

Theorem 1 gives an asymptotic formula for the number of $n < x$ such that $a_n \neq 0$ but says nothing about the number of $n < x$ such that $a_n = a$, where a is a specific fixed value in \mathbb{F}^* . Some partial results are given during the course of the proof of Theorem 1 in Section 4A. We say that f has the *equidistribution property* if the number of $n < x$ such that $a_n = a$ is asymptotically the same for every $a \in \mathbb{F}^*$. In Section 5 we give sufficient conditions and, in some cases, necessary conditions for the equidistribution property.

In Section 6 we consider a variant of the main theorem, where one counts only the nonzero coefficients at square-free integers of a modular form.

Let us finally mention that the constants $\alpha(f)$, $h(f)$ and $c(f)$ of Theorem 1 can be effectively computed from our proof. This is done in some cases in Section 7. However, we do not have a satisfactory understanding of how $h(f)$ and $c(f)$ behave as f varies. Such an understanding would require a more detailed study of the structure of the Hecke algebra A and of the space $M(N, \mathbb{F})$ as a Hecke-module than is currently available (except in the case $p = 2$, $N = 1$ [Nicolas and Serre 2012b; Bellaïche and Nicolas 2015] and partially in the case $p = 3$, $N = 1$ [Medvedovki 2015]).

2. Applications of the Landau–Selberg–Delange method

2A. Frobenian and multifrobenian sets. If Σ is a finite set of primes and L is a finite Galois extension of \mathbb{Q} unramified outside Σ and ∞ , then for any prime $\ell \notin \Sigma$ we denote by $\text{Frob}_\ell \in \text{Gal}(L/\mathbb{Q})$ an element of Frobenius attached to ℓ . We recall that Frob_ℓ is only well-defined up to conjugation in $\text{Gal}(L/\mathbb{Q})$.

Definition 2. Let h be a nonnegative integer and Σ a finite set of primes. We say that a set \mathcal{M} of positive integers is Σ -multifrobenian of height h if there exists a finite Galois extension L of \mathbb{Q} with Galois group G , unramified outside Σ and ∞ , and a subset D of G^h , invariant under conjugation and under permutations of the coordinates, such that $m \in \mathcal{M}$ if and only if $m = \ell_1 \cdots \ell_h$ where the ℓ_i are distinct primes not in Σ , and $(\text{Frob}_{\ell_1}, \dots, \text{Frob}_{\ell_h}) \in D$. For such a Σ -multifrobenian set \mathcal{M} we define its density $\delta(\mathcal{M})$ to be

$$\delta(\mathcal{M}) = \frac{\#\mathcal{M}}{h!(\#G)^h}.$$

Observe that the condition $(\text{Frob}_{\ell_1}, \dots, \text{Frob}_{\ell_h}) \in D$ depends only on the product $\ell_1 \cdots \ell_h$, since replacing each Frob_{ℓ_i} by a conjugate in G amounts to replacing $(\text{Frob}_{\ell_1}, \dots, \text{Frob}_{\ell_h})$ by a conjugate in G^h and D is invariant by conjugacy in G^h , and since changing the order of the prime factors ℓ_1, \dots, ℓ_h permutes the components of $(\text{Frob}_{\ell_1}, \dots, \text{Frob}_{\ell_h})$ and D is invariant by permutations. Thus the notion of a multifrobenian set is well-defined.

There is only one Σ -multifrobenian set of height $h = 0$, namely $\{1\}$. Note that a Σ -multifrobenian set of height 1 is just a Σ -frobenian set of prime numbers in the usual sense (see [Serre 2012, §3.3.1]). In what follows we will say that a set is *multifrobenian* if it is Σ -multifrobenian for some finite set of primes Σ and *frobenian* if it is multifrobenian of height 1. We observe that this definition of frobenian is slightly more restrictive than the one used by Serre (cf. [2012, §3.3.2]) for whom a set of primes is frobenian if it is frobenian in our sense up to a finite set of primes. The more restrictive definition of frobenian that we adopt here will be sufficient for our purposes, and we hope that its use will cause no confusion to the reader.

Lemma 3. *Let \mathcal{M} be a multifrobenian set of height h and density $\delta(\mathcal{M})$. Then*

$$\sum_{\substack{m \in \mathcal{M} \\ m \leq x}} \frac{1}{m} \sim \delta(\mathcal{M})(\log \log x)^h.$$

Proof. This follows from the Chebotarev density theorem. □

Note in particular that $\delta(\mathcal{M})$ depends only on the set \mathcal{M} and not on the choice of L , G and D .

Remark 4. Using the Chebotarev density theorem, one may show that if \mathcal{M} is a multifrobenian set of height h , then

$$|\{n \leq x : n \in \mathcal{M}\}| \sim h\delta(\mathcal{M}) \frac{x}{\log x} (\log \log x)^{h-1}.$$

This formula clearly implies Lemma 3 by partial summation, but the weaker Mertens-type estimate of Lemma 3 suffices for our purposes.

2B. Square-free integers with prime factors in a frobenian set and random walks. We begin with a general result of the Landau–Selberg–Delange type, which follows by the method discussed in Chapter II.5 of Tenenbaum’s book [1995], or as in Théorème 2.8 of Serre’s paper [1976].

Proposition 5. *Let $a(n)$ be a sequence of complex numbers with $|a(n)| \leq d_k(n)$ for some natural number k , where $d_k(n)$ denotes the k -divisor function defined by $\zeta(s)^k = \sum_{n=1}^{\infty} d_k(n)n^{-s}$. Suppose that in the region $\operatorname{Re}(s) > 1$ the function $A(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ can be written, for some real number α , as*

$$A(s) = \zeta(s)^\alpha B(s),$$

where $B(s)$ extends analytically to the region $\operatorname{Re}(s) > 1 - c/\log(2 + |t|)$ for some positive constant c and is bounded in that region by $|B(s)| \leq C(1 + |t|)$ for some constant C . Then, for all $x \geq 3$ and any $J \geq 0$, there is an asymptotic expansion

$$\sum_{n \leq x} a(n) = \sum_{j=0}^J \frac{A_j x}{(\log x)^{1+j-\alpha}} + O\left(\frac{Cx}{(\log x)^{J+2-\alpha}}\right),$$

where the A_j are constants, with

$$A_0 = \frac{B(1)}{\Gamma(\alpha)},$$

and the implied constant in the remainder term depends only on c , k , and J .

Proof. As mentioned above, this is a straightforward application of the Landau–Selberg–Delange method, and so we content ourselves with sketching the argument briefly. The constant c can be replaced by a possibly smaller constant so that $\zeta(s)$ has no zeros in the region $\operatorname{Re}(s) > 1 - c/\log(2 + |t|)$, and moreover in this region we have the classical bounds $|\zeta(s)^\alpha| \ll (\log(|s| + 2))^{A|\alpha|}$ for some constant A provided we stay away from $s = 1$ (see for example II.3 of [Tenenbaum 1995]). Next, by applying a quantitative version of Perron’s formula we see that, for $x \geq 3$ and with $x^{1/(10k)} \geq T \geq 1$,

$$\sum_{n \leq x} a(n) = \frac{1}{2\pi i} \int_{1+1/\log x - iT}^{1+1/\log x + iT} A(s) \frac{x^s}{s} ds + O\left(\frac{x}{T} (\log x)^k\right).$$

Now we deform the line of integration as follows. First make a slit along the real line segment from $1 - c/\log(T + 2)$ to 1 . Then from $1 + 1/\log x + iT$ we proceed in a straight line to $1 - c/\log(T + 2) + iT$ and from there to $1 - c/\log(T + 2) + i0^+$ (on the upper part of the slit) and from there to 1 . We then circle around to the lower part of the slit until $1 - c/\log(T + 2) + i0^-$ and from there to $1 - c/\log(T + 2) - iT$ and thence to $1 + 1/\log x - iT$. The integrand has a logarithmic singularity at 1 , and the change in the argument above and below the slit leads to the main terms in the asymptotic expansion (by ‘‘Hankel’s formula’’; see [Tenenbaum 1995, §II.5.2]). The remaining integrals are estimated using the bounds for $|\zeta(s)^\alpha|$ in the zero-free region, together with our assumed bound for $|B(s)|$. The resulting error terms are bounded by $O(x^{1-c/\log(T+2)}(T+2)\log(T+2))$. Choosing $T = \exp(c_1\sqrt{\log x})$ for a suitably small positive constant c_1 , we obtain the proposition. \square

Now suppose we are given a frobenian set of primes \mathcal{U} of density $\beta = \delta(\mathcal{U}) > 0$, a finite abelian group Γ , and a frobenian map³ $\tau_0 : \mathcal{U} \rightarrow \Gamma$ such that the image $\tau_0(\mathcal{U})$ generates Γ . Using multiplicativity, extend τ_0 to a map τ from the set of square-free numbers composed of prime factors in \mathcal{U} to Γ .

Theorem 6. *Let g be any given element of Γ , and let r be a positive integer. Then, for $x \geq 3$ and uniformly in r , we have*

$$\begin{aligned} \#\{n \leq x : n \text{ square-free}, p \mid n \implies p \in \mathcal{U}, \tau(n) = g, (n, r) = 1\} \\ = C(\mathcal{U}, r) \frac{1}{|\Gamma|} \frac{x}{(\log x)^{1-\beta}} + O\left(\frac{xd(r)}{(\log x)^{1-\beta+\delta}}\right), \end{aligned}$$

where $C(\mathcal{U}, r) = (1/\Gamma(\beta)) \prod_p w_p$ with $w_p = (1 + 1/p)(1 - 1/p)^\beta$ if $p \in \mathcal{U}$ with $p \nmid r$, and $w_p = (1 - 1/p)^\beta$ otherwise. In the remainder term above, $d(r)$ denotes the number of divisors of r , and δ is a fixed positive number (depending only on the group Γ).

Proof. We use the orthogonality of the characters of the group Γ , which we write multiplicatively even though it is abelian. Thus the quantity we want is

$$\frac{1}{|\Gamma|} \sum_{\chi \in \widehat{\Gamma}} \overline{\chi(g)} \sum_{\substack{n \leq x \\ (n,r)=1}} \chi(\tau(n)),$$

where we set $\chi(\tau(n)) = 0$ if n is divisible by some prime not in \mathcal{U} or if n is not square-free.

We will use Proposition 5 to evaluate the sum over n above. Since the map τ is frobenian, by the usual proof of the Chebotarev density theorem (that is, by expressing frobenian sets in terms of Hecke L -functions and using the zero-free

³A map from a frobenian set of primes to a finite set is called *frobenian* if its fibers are frobenian.

region for Hecke L -functions) we may write

$$\sum_{\substack{n=1 \\ (n,r)=1}}^{\infty} \frac{\chi(\tau(n))}{n^s} = \zeta(s)^{\beta(\chi)} B_{\chi,r}(s), \quad \text{where } \beta(\chi) = \sum_{g \in \Gamma} \chi(g) \delta(\tau_0^{-1}(g)),$$

and $B_{\chi,r}(s)$ extends analytically to the region $\text{Re}(s) > 1 - c/(\log(2 + |t|))$ for some $1/10 \geq c > 0$ and in that region satisfies the bound $|B_{\chi,r}(s)| \leq Cd(r)(1 + |t|)$ for some constant C . The constants c and C depend only on \mathcal{U} and Γ but not on r .

First suppose that χ equals the trivial character χ_0 . Note that $\beta(\chi)$ then equals β and that

$$B_{\chi_0,r}(s) = \prod_{\substack{p \in \mathcal{U} \\ p \nmid r}} \left(1 - \frac{1}{p^s}\right)^\beta \left(1 + \frac{1}{p^s}\right) \prod_{\substack{p \notin \mathcal{U} \\ \text{or } p \mid r}} \left(1 - \frac{1}{p^s}\right)^\beta.$$

Therefore, appealing to Proposition 5, we obtain the main term of the theorem.

Now suppose that χ is not the trivial character. Then $\text{Re}(\beta(\chi)) \leq \beta - \delta$ for some fixed $\delta > 0$, since there is a g in the image of τ_0 such that $\chi(g) \neq 1$ (since $\tau(\mathcal{U})$ generates Γ), and the frobenian set $\tau_0^{-1}(g)$ is nonempty and hence of positive density $\delta(\tau_0^{-1}(g))$. Therefore, by Proposition 5, we see that the contribution of the nontrivial characters is

$$O\left(\frac{xd(r)}{(\log x)^{1-\beta+\delta}}\right). \quad \square$$

2C. A density result. We keep the notation and hypotheses of the preceding section: \mathcal{U} is a frobenian set with $\beta = \delta(\mathcal{U}) > 0$, Γ is a finite abelian group, and $\tau_0 : \mathcal{U} \rightarrow \Gamma$ is a frobenian map whose image generates Γ . In addition, let \mathcal{M} be a multifrobenian set of height $h \geq 0$, such that every element in \mathcal{M} is coprime to the primes in \mathcal{U} . Let \mathcal{S} be a given nonempty set of square-full numbers (we permit 1 to be treated as a square-full number).

Define $\mathcal{Z} = \mathcal{Z}(\mathcal{U}, \mathcal{M}, \mathcal{S})$ to be the set of positive integers $n \geq 1$ that can be written as

$$(2.1) \quad n = mm'm'' \text{ with } m, m', m'' \text{ positive integers such that}$$

$$(2.1.1) \quad m \text{ is square-free and all its prime factors are in } \mathcal{U};$$

$$(2.1.2) \quad m' \in \mathcal{M};$$

$$(2.1.3) \quad m'' \in \mathcal{S} \text{ and } m'' \text{ is relatively prime to } mm'.$$

These conditions imply that m, m' and m'' are pairwise relatively prime, and for $n \in \mathcal{Z}$ such a decomposition $n = mm'm''$ is unique. Extend τ to a map $\mathcal{Z} \rightarrow \Gamma$ by setting $\tau(n) = \tau(m)$ for n as in (2.1). Let Δ be any nonempty subset of Γ .

Theorem 7. *With notation as above, we have*

$$\#\{n \leq x : n \in \mathcal{Z}, \tau(n) \in \Delta\} \sim C\delta(\mathcal{M}) \frac{|\Delta|}{|\Gamma|} \frac{x}{(\log x)^{1-\beta}} (\log \log x)^h,$$

where (with $C(\mathcal{U}, s)$ as in Theorem 6)

$$C = \sum_{s \in \mathcal{S}} \frac{C(\mathcal{U}, s)}{s}.$$

Proof. Set $R = (\log x)^2$ and $z = x^{1/\log \log x}$. We want to count $n = mm'm''$ for $m'' \in \mathcal{S}$, $m' \in \mathcal{M}$, with $(m', m'') = 1$, and for m composed of primes in \mathcal{U} , with $(m, m'') = 1$ and $\tau(m) = g$. We now group these terms according to whether (i) $m'' \leq R$ and $m' \leq z$, or (ii) $m'' \leq R$ but $m' > z$, or (iii) $m'' > R$. We shall show that the first case gives the main term in the asymptotics, and the other two cases are negligible.

First consider case (i). This case contributes

$$\sum_{\substack{m'' \in \mathcal{S} \\ m'' \leq R}} \sum_{\substack{m' \in \mathcal{M} \\ m' \leq z \\ (m', m'')=1}} \sum_{g \in \Delta} \left| \left\{ m \leq \frac{x}{m'm''} : \tau(m) = g, (m, m'') = 1 \right\} \right|.$$

Now we use Theorem 6, so that the above equals

$$\sum_{\substack{m'' \in \mathcal{S} \\ m'' \leq R}} \sum_{\substack{m' \in \mathcal{M} \\ m' \leq z \\ (m', m'')=1}} \left(C(\mathcal{U}, m'') \frac{|\Delta|}{|\Gamma|} \frac{x}{m'm''(\log(x/m'm''))^{1-\beta}} + O\left(\frac{xd(m'')}{m'm''(\log x)^{1-\beta+\delta}}\right) \right).$$

Using Lemma 3, and since $\sum_{m'' \in \mathcal{S}} d(m'')/m''$ converges, we see that the error term above is $O(x/(\log x)^{1-\beta+\delta-\epsilon})$, which is negligible. Since $\log(x/m'm'') \sim \log x$, the main term above is (again using Lemma 3)

$$\sim \frac{|\Delta|}{|\Gamma|} \frac{x}{(\log x)^{1-\beta}} (\delta(\mathcal{M})(\log \log x)^h) \sum_{\substack{m'' \in \mathcal{S} \\ m'' \leq R}} \frac{C(\mathcal{U}, m'')}{m''},$$

which equals the main term of the theorem.

Now consider case (ii). Since all the terms involved are positive, we see that they contribute (with $\omega(u)$ denoting the number of distinct prime factors of u)

$$\ll \sum_{\substack{m'' \in \mathcal{S} \\ m'' \leq R}} \sum_{\substack{z \leq u \leq x/m'' \\ \omega(u)=h}} \sum_{\substack{m \leq x/(um'') \\ p|m \Rightarrow p \in \mathcal{U}}} 1. \tag{4}$$

Now in the sums above either $u \leq \sqrt{x}$ or $m \leq \sqrt{x}$. In the first case, note that the largest prime factor of u lies in $[z^{1/h}, \sqrt{x}]$ and the others are all below \sqrt{x} . Moreover, using Proposition 5, the inner sum over m in (4) is $\ll x/(um''(\log x)^{1-\beta})$.

Thus we see that the first-case contribution to (4) is bounded by

$$\begin{aligned} &\ll \sum_{\substack{m'' \in \mathcal{S} \\ m'' \leq R}} \sum_{\substack{z < u \leq \sqrt{x} \\ \omega(u) = h}} \frac{x}{um''(\log x)^{1-\beta}} \ll \frac{x}{(\log x)^{1-\beta}} \left(\sum_{\substack{p \geq z^{1/h} \\ p \leq \sqrt{x}}} \frac{1}{p} \right) \left(\sum_{p \leq \sqrt{x}} \frac{1}{p} \right)^{h-1} \\ &\ll \frac{x}{(\log x)^{1-\beta}} (\log \log x)^{h-1} \log \log \log x. \end{aligned}$$

For the second case, note that for $m \leq \sqrt{x}$ (and $m'' \leq R = (\log x)^2$) we have (by standard estimates for the number of integers with h distinct prime factors)

$$\sum_{\substack{u \leq x/(mm'') \\ \omega(u) = h}} 1 \ll \frac{x}{mm''} \frac{(\log \log x)^{h-1}}{\log x},$$

and so we obtain that the second-case contribution to (4) is bounded by

$$\begin{aligned} &\ll \frac{x}{\log x} (\log \log x)^{h-1} \sum_{\substack{m \leq \sqrt{x} \\ m \in \mathcal{U}}} \frac{1}{m} \ll \frac{x}{\log x} (\log \log x)^{h-1} \prod_{\substack{p \leq \sqrt{x} \\ p \in \mathcal{U}}} \left(1 + \frac{1}{p} \right) \\ &\ll \frac{x}{(\log x)^{1-\beta}} (\log \log x)^{h-1}. \end{aligned}$$

Putting both cases together, we see that the contribution of the terms in case (ii) is

$$\ll \frac{x}{(\log x)^{1-\beta}} (\log \log x)^{h-1} \log \log \log x,$$

which is small compared to the contribution from case (i).

Finally, since the number of $mm' \leq x/m''$ is trivially at most x/m'' , the contribution in case (iii) is

$$\ll \sum_{\substack{m'' \in \mathcal{S} \\ m'' > R}} \frac{x}{m''} \ll \frac{x}{\sqrt{R}} = \frac{x}{\log x},$$

which is negligible. This completes our proof. □

3. Modular forms modulo p

3A. The algebra of modular forms $M(N, \mathbb{F})$. As in the introduction, we fix an odd prime p and a level $N \geq 1$. Let $k \geq 0$ be an integer. The space $M_k(N, \mathbb{Z})$ denotes the space of all holomorphic modular forms of weight k and level $\Gamma_1(N)$ and with q -expansion at infinity in $\mathbb{Z}[[q]]$. For any commutative ring A we define

$$M_k(N, A) = M_k(N, \mathbb{Z}) \otimes A.$$

The natural q -expansion map $M_k(N, A) \rightarrow A[[q]]$ is injective for any ring A (this is the q -expansion principle; see [Diamond and Im 1995, Theorem 12.3.4]), and so we may view below $M_k(N, A)$ as a subspace of $A[[q]]$. Finally we define

$$M(N, A) = \sum_{k=0}^{\infty} M_k(N, A) \subset A[[q]].$$

Note that if A is a subring of \mathbb{C} , then $M(N, A)$ is the *direct* sum of the spaces $M_k(N, A)$ (see [Miyake 2006, Lemma 2.1.1]). However, the situation is different for general rings A and, in particular, when A is a finite field. For instance, the constant modular form 1 of weight 0 in $M_0(N, \mathbb{F}_p)$ and the Eisenstein series E_{p-1} in $M_{p-1}(N, \mathbb{F}_p)$ both have the same q -expansion 1, showing that the subspaces $M_0(N, \mathbb{F}_p)$ and $M_{p-1}(N, \mathbb{F}_p)$ are not in direct sum in $\mathbb{F}_p[[q]]$. For the same reason it is not true that $M(N, A) \otimes_A A' = M(N, A')$ in general (though this is true if A' is flat over A); rather $M(N, A')$ is the image of $M(N, A) \otimes_A A'$ in $A'[[q]]$.

3B. Hecke operators on $M_k(N, A)$. For any $k \geq 0$, the space of modular forms $M_k(N, \mathbb{C})$ is endowed with the action of the Hecke operators T_n for positive integers n . If n is a positive integer coprime to N , define the operator S_n as $n^{k-2}\langle n \rangle$, where $\langle n \rangle$ is the diamond operator. Recall that these operators satisfy the following properties.

- (3.1) All the operators T_n and S_m commute.
- (3.2) We have $S_1 = 1$ and $S_{mn} = S_m S_n$ for all m, n coprime to N .
- (3.3) The Hecke relations $T_1 = 1$, $T_{mn} = T_m T_n$ if $(m, n) = 1$ hold. If $\ell \nmid N$ is prime, then $T_{\ell^{n+1}} = T_{\ell^n} T_{\ell} - \ell S_{\ell} T_{\ell^{n-1}}$. If $\ell \mid N$ is prime then $T_{\ell^n} = (T_{\ell})^n$.

As is customary, we shall also use below the notation U_{ℓ} for the operators T_{ℓ} when $\ell \mid N$. From the above relations one sees that the operators T_{ℓ} and S_{ℓ} for ℓ prime determine all the others. Recall that the action of the Hecke operators on q -expansions is given as follows.

- (3.4) If $\ell \mid N$ then $a_n(U_{\ell} f) = a_{\ell n}(f)$.
- (3.5) If $\ell \nmid N$ is prime, then $a_n(T_{\ell} f) = a_{\ell n}(f) + \ell a_{n/\ell}(S_{\ell} f)$, with the understanding that $a_{n/\ell}$ means 0 if $\ell \nmid n$.

It follows that

- (3.6) if $(n, m) = 1$ then $a_n(T_m f) = a_{nm}(f)$; in particular, $a_1(T_m f) = a_m(f)$ for every $m \geq 1$.

Lastly, we recall the following important fact, which follows from the geometric interpretation due to Katz [1973] of the elements of $M_k(N, A)$ as the sections of a coherent sheaf on the modular curve $Y_1(N)_{/A}$ over A , and of the Hecke operators

as correspondences on $Y_1(N)$. A convenient reference is [Diamond and Im 1995, Chapter 12].

(3.7) Let A be a subring of \mathbb{C} . All the operators T_n and S_n leave stable the subspace $M_k(N, A)$ of $M_k(N, \mathbb{C})$.

This fact allows us to define unambiguously the operators T_n and S_n over $M_k(N, A) = M_k(N, \mathbb{Z}) \otimes_{\mathbb{Z}} A$ by extending the scalars from \mathbb{Z} to A for the linear operators T_n and S_n on $M_k(N, \mathbb{Z})$.

3C. Hecke operators on $M(N, \mathbb{F})$. From now on, \mathbb{F} is a finite field of characteristic p . First we recall a result due to Serre and Katz, which allows us to assume that the level N is prime to p ; for a proof, see [Gouvêa 1988, pages 21–22].

(3.8) Let \mathbb{F} be a finite field of characteristic p . Write $N = N_0 p^v$ with $(N_0, p) = 1$. Then as subspaces of $\mathbb{F}[[q]]$ one has $M(N, \mathbb{F}_p) = M(N_0, \mathbb{F}_p)$.

Henceforth, we assume that $(N, p) = 1$.

(3.9) There are unique operators T_n (for any $n \geq 1$) and S_n (for $n \geq 1$ with $(n, N) = 1$) on $M(N, \mathbb{F})$ such that, for any $k \geq 0$, the inclusion $M_k(N, \mathbb{F}) \hookrightarrow M(N, \mathbb{F})$ is compatible with the operators T_n and S_n defined on the source and target.

Since the sum of the $M_k(N, A)$ for $k = 0, 1, 2, \dots$ is $M(N, A)$ by definition, the uniqueness claimed in (3.9) follows. The existence relies on the interpretation of the elements of $M(N, A)$ as algebraic functions on the open Igusa curve (an étale cover of degree $p - 1$ of the ordinary locus of $Y_1(N)_{/\mathbb{F}_p}$) which is due to Katz (see [1973; 1975, Theorem 2.2]) and based on earlier work of Igusa. For a more recent reference for (3.9), see [Gross 1990, Propositions 5.5 and 5.9].

It is clear that the operators T_n and S_n still satisfy properties (3.1) to (3.6). We record one more easy consequence of (3.9).

(3.10) The actions of the Hecke operators T_n and S_n on $M(N, \mathbb{F})$ are locally finite. That is, any form $f \in M(N, \mathbb{F})$ is contained in a finite-dimensional subspace of $M(N, \mathbb{F})$ stable under all these operators.

We shall use the notation U_p instead of T_p when acting on the space $M(N, \mathbb{F})$. More generally, if m is an integer all of whose prime factors divide Np we shall use the notation U_m instead of T_m .

Finally, we note that the space $M(N, \mathbb{F})$ enjoys an additional Hecke operator (see [Jochnowitz 1982, §1]).

(3.11) The subspace $M(N, \mathbb{F})$ of $\mathbb{F}[[q]]$ is stable under the operator V_p defined by
$$V_p\left(\sum a_n q^n\right) = \sum a_n q^{pn}.$$

3D. The subspace $\mathcal{F}(N, \mathbb{F})$ of $M(N, \mathbb{F})$. Using the same notation as in [Nicolas and Serre 2012a; 2012b], let us define $\mathcal{F}(N, \mathbb{F})$ as the subspace $\bigcap_{\ell|Np} \ker U_\ell$ of $M(N, \mathbb{F})$. In other words,

$$(3.12) \quad \mathcal{F}(N, \mathbb{F}) = \{f = \sum_{n=0}^\infty a_n q^n \in M(N, \mathbb{F}), a_n \neq 0 \Rightarrow (n, Np) = 1\}.$$

Since the Hecke operators commute, T_ℓ and S_ℓ for $\ell \nmid Np$ stabilize $\mathcal{F}(N, \mathbb{F})$.

3E. The residual Galois representations $\bar{\rho}$ and the invariant $\alpha(\bar{\rho})$. We denote by $G_{\mathbb{Q}, Np}$ the Galois group of the maximal algebraic extension of \mathbb{Q} unramified outside Np . We denote by c a complex conjugation in $G_{\mathbb{Q}, Np}$. If ℓ is a prime not dividing Np , we denote by Frob_ℓ an element of Frobenius associated to ℓ in $G_{\mathbb{Q}, Np}$. We fix an algebraic closure $\bar{\mathbb{F}}_p$ of \mathbb{F}_p .

We shall denote by $R = R(N, p)$ the set of equivalence classes of continuous odd⁴ semisimple two-dimensional representations $\bar{\rho}$ of the Galois group $G_{\mathbb{Q}, Np}$ over $\bar{\mathbb{F}}_p$ that are attached to eigenforms in $M(N, \bar{\mathbb{F}}_p)$. Here we say that $\bar{\rho}$ is attached to an eigenform in $M(N, \bar{\mathbb{F}}_p)$ if there exists a nonzero eigenform $f \in M(N, \bar{\mathbb{F}}_p)$ for the Hecke operators T_ℓ and S_ℓ for $\ell \nmid Np$, with eigenvalues λ_ℓ and σ_ℓ , such that

$$(3.13) \quad \text{the characteristic polynomial of } \bar{\rho}(\text{Frob}_\ell) \text{ is } X^2 - \lambda_\ell X + \ell\sigma_\ell.$$

Although we do not need this fact, we remark that Khare and Wintenberger have shown Serre’s conjecture that every odd semisimple two-dimensional representation of Serre’s conductor N is attached to an eigenform in $M(N, \bar{\mathbb{F}}_p)$.

A result of Atkin, Serre and Tate in the case $N = 1$ [Serre 1973], and of Jochnowitz in the general case [1982, Theorem 2.2], states that the number of systems of eigenvalues for the T_ℓ and S_ℓ appearing in $M(N, \bar{\mathbb{F}}_p)$ is finite. Hence $R(N, p)$ is a finite set. If $\bar{\rho} : G_{\mathbb{Q}, Np} \rightarrow \text{GL}_2(\bar{\mathbb{F}}_p)$ is a representation, it is defined over some finite extension \mathbb{F} of \mathbb{F}_p inside $\bar{\mathbb{F}}_p$ (for absolutely irreducible $\bar{\rho}$, this amounts to saying that $\text{tr } \bar{\rho}(G_{\mathbb{Q}, Np}) \subset \mathbb{F}$, since finite fields have trivial Brauer groups). Therefore, there exists a finite extension \mathbb{F} of \mathbb{F}_p such that all representations in $R(N, p)$ are defined over \mathbb{F} .

For $\bar{\rho} \in R(N, p)$, we shall denote by $U_{\bar{\rho}}$ the open and closed subset of $G_{\mathbb{Q}, Np}$ of elements g such that $\text{tr } \bar{\rho}(g) \neq 0$, and by $N_{\bar{\rho}}$ its complement, the set of elements g such that $\text{tr } \bar{\rho}(g) = 0$. We set $\alpha(\bar{\rho}) = \mu_{G_{\mathbb{Q}, Np}}(N_{\bar{\rho}})$, where $\mu_{G_{\mathbb{Q}, Np}}$ is the Haar measure on the compact group $G_{\mathbb{Q}, Np}$.

Proposition 8. *For all representations $\bar{\rho}$ we have $\alpha(\bar{\rho}) \in \mathbb{Q}$ with $0 < \alpha(\bar{\rho}) \leq 3/4$. If $\bar{\rho}$ is reducible, we have $\alpha(\bar{\rho}) \leq 1/2$.*

Proof. By definition, $\alpha(\bar{\rho})$ is the proportion of elements of trace zero in the finite subgroup $G = \bar{\rho}(G_{\mathbb{Q}, Np})$ of $\text{GL}_2(\bar{\mathbb{F}}_p)$. Thus $\alpha(\bar{\rho})$ is rational and is at most one. Since $\bar{\rho}(c)$ has trace zero, we have $\alpha(\bar{\rho}) > 0$. It remains now to obtain the upper

⁴That is, such that $\text{tr } \bar{\rho}(c) = 0$.

bounds claimed for $\alpha(\bar{\rho})$. Let G' be the image of G in $\text{PGL}_2(\bar{\mathbb{F}}_p)$. Then $\alpha(\bar{\rho})$ is also the proportion of elements of trace zero in G' (it makes sense to say that an element of $\text{PGL}_2(\bar{\mathbb{F}}_p)$ has “trace zero”, even though the trace of such an element is of course not well-defined). Also, observe that an element g' in $\text{PGL}_2(\bar{\mathbb{F}}_p)$ has trace 0 if and only if it has order exactly 2. Indeed, let g be a lift of g' in $\text{GL}_2(\bar{\mathbb{F}}_p)$. If g is diagonalizable and x, y are its eigenvalues, then g' having order exactly 2 means that $x \neq y$, but $x^2 = y^2$; thus $x = -y$, and $\text{tr } g = 0$. If g is not diagonalizable, then the order of g' is a power of p , hence not 2, and it has a double eigenvalue $x \neq 0$ so its trace $2x$ is not 0. Hence $\alpha(\bar{\rho})$ is also the proportion of elements of order 2 in G' .

If $\bar{\rho}$ is reducible, then, since $\bar{\rho}$ is assumed semisimple, G is conjugate to a subgroup of the diagonal subgroup $D = \bar{\mathbb{F}}_p^* \times \bar{\mathbb{F}}_p^*$, and G' may thus be assumed to be a subgroup of the image D' of D in PGL_2 . The group D' is isomorphic to $\bar{\mathbb{F}}_p^*$, by the isomorphism sending $x \in \bar{\mathbb{F}}_p^*$ to the image of $\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}$ in $\text{PGL}_2(\bar{\mathbb{F}}_p)$, and via this identification the only element of trace zero of D' is -1 , which is always in G' because G contains $\bar{\rho}(c)$. Thus one has $\alpha(\bar{\rho}) = 1/|G'|$. Therefore, $\alpha(\bar{\rho}) \leq 1/2$ since G' is not the trivial group because $\bar{\rho}(c)$ is not trivial in $\text{PGL}_2(\bar{\mathbb{F}}_p)$.

Now assume that $\bar{\rho}$ is irreducible. We shall use the classification of subgroups of $\text{PGL}_2(\bar{\mathbb{F}}_p)$ for which a convenient modern reference is [Faber 2012]. According to Theorems B and C of [Faber 2012], if G' is any finite subgroup of $\text{PGL}_2(\bar{\mathbb{F}}_p)$, we are in one of the 9 situations described there and labeled B(1) to B(4) and C(1) to C(5). The case B(3) does not arise since we assume $p > 2$, and neither do cases B(2) and C(1) which contradict the assumed irreducibility of $\bar{\rho}$ (for B(2) because G' cyclic implies G abelian, and for C(1) by Remark 2.1 of [Faber 2012]). In the other situations, we argue as follows.

C(2) G' is isomorphic to a dihedral group D_{2n} of order $2n$ (for $n \geq 2$ an integer) which is a semidirect product of a cyclic group C_n by a subgroup of order 2. In this case, the elements of order 2 are the elements not in C_n and, if n is even, the unique element of order 2 in C_n . Thus

$$\alpha(\bar{\rho}) = \begin{cases} \frac{1}{2} & \text{if } n \text{ is odd,} \\ \frac{1}{2} + \frac{1}{2n} & \text{if } n \text{ is even.} \end{cases}$$

Note that if $n = 2$, then $\alpha(\bar{\rho}) = 3/4$, and in all other cases $\alpha(\bar{\rho}) \leq 5/8$.

C(3) $G' \simeq A_4$, so $\alpha(\bar{\rho}) = 1/4$ since A_4 has order 12, and has 3 elements of order 2.

C(4) $G' \simeq S_4$, so $\alpha(\bar{\rho}) = 3/8$ since S_4 has order 24 and 9 elements of order 2 (6 transpositions and 3 products of two disjoint transpositions).

C(5), B(4) $G' \simeq A_5$, so $\alpha(\bar{\rho}) = 1/4$ since A_5 has order 60 and has 15 elements of order 2 (the products of two disjoint transpositions).

B(1) The subgroup G' of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ is conjugate to $\mathrm{PGL}_2(\mathbb{F}_q)$, where q is some power of p . In this case, the number of matrices of trace 0 in G' is q^2 , while $|G'| = q(q-1)(q+1)$, so

$$\alpha(\bar{\rho}) = \frac{q}{(q-1)(q+1)}.$$

Thus in this case we have $\alpha(\bar{\rho}) \leq 3/8$, and this bound is attained for $q = 3$.

B(1) again The subgroup G' of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ is conjugate to $\mathrm{PSL}_2(\mathbb{F}_q)$. The number of matrices of trace 0 in $\mathrm{SL}_2(\mathbb{F}_q)$ is $q^2 - q$ if -1 is not a square in \mathbb{F}_q and $q^2 + q$ if -1 is a square. Since $|\mathrm{SL}_2(\mathbb{F}_q)| = q(q-1)(q+1)$ one has

$$\alpha(\bar{\rho}) = \begin{cases} \frac{1}{q+1} & \text{if } -1 \text{ is not a square in } \mathbb{F}_q, \\ \frac{1}{q-1} & \text{if } -1 \text{ is a square in } \mathbb{F}_q. \end{cases}$$

Thus in this case we have $\alpha(\bar{\rho}) \leq 1/4$, and this value is attained for $q = 3$ and $q = 5$. □

3F. The Hecke algebra A . From now on, we assume that \mathbb{F} is a finite field contained in $\overline{\mathbb{F}}_p$ and large enough to contain the fields of definition of all the representations $\bar{\rho} \in R(N, p)$.

Let $A = A(N, \mathbb{F})$ be the closed subalgebra of $\mathrm{End}_{\mathbb{F}}(M(N, \mathbb{F}))$ generated by the Hecke operators T_ℓ and S_ℓ for ℓ prime not dividing Np . Equivalently, by (3.3), A is the closed subalgebra of $\mathrm{End}_{\mathbb{F}}(M(N, \mathbb{F}))$ generated by the T_m for all m relatively prime to Np . Here we give $M(N, \mathbb{F})$ its discrete topology and $\mathrm{End}_{\mathbb{F}}(M(N, \mathbb{F}))$ its compact-open topology. Then $M = M(N, \mathbb{F})$ and $\mathcal{F} = \mathcal{F}(N, \mathbb{F})$ are topological A -modules. Note that if $f \in M$ (or if $f \in \mathcal{F}$) the submodule Af of M (respectively of \mathcal{F}) generated by f is finite-dimensional over \mathbb{F} by (3.10), and hence is finite as a set.

By construction, the maximal ideals of $A(N, \mathbb{F})$ correspond to the $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F})$ -conjugacy classes of systems of eigenvalues (for the T_ℓ and S_ℓ , $\ell \nmid Np$) appearing in $M(N, \overline{\mathbb{F}}_p)$. As recalled earlier, the set of such systems is finite and in natural bijection (determined by the Eichler–Shimura relation (3.13)) with the set $R(N, p)$. Further, by our choice of \mathbb{F} , all those eigenvalues are in \mathbb{F} . It follows that A is a semilocal ring; more precisely, we have a natural decomposition

$$A = \prod_{\bar{\rho} \in R(N, p)} A_{\bar{\rho}},$$

where $A_{\bar{\rho}}$ is the localization of A at the maximal ideal corresponding to the system of eigenvalues corresponding to $\bar{\rho}$. The quotient $A_{\bar{\rho}}$ of A is a complete local \mathbb{F} -algebra of residue field \mathbb{F} , and if one denotes by $T_{\bar{\rho}}$ the image of an element $T \in A$

in $A_{\bar{\rho}}$, then $A_{\bar{\rho}}$ is characterized among the local components of A by the following property.

(3.14) For every $\ell \nmid Np$, the elements $T_{\ell, \bar{\rho}} - \text{tr } \bar{\rho}(\text{Frob}_\ell)$ and $\ell S_\ell - \det \bar{\rho}(\text{Frob}_\ell)$ belong to the maximal ideal $\mathfrak{m}_{\bar{\rho}}$ of $A_{\bar{\rho}}$ (or, equivalently, are topologically nilpotent in $A_{\bar{\rho}}$).

The decomposition of A as $\prod A_{\bar{\rho}}$ gives rise to corresponding decompositions of $M = M(N, \mathbb{F})$ and $\mathcal{F} = \mathcal{F}(N, \mathbb{F})$:

$$M = \bigoplus_{\bar{\rho} \in R(N, p)} M_{\bar{\rho}}, \quad \mathcal{F} = \bigoplus_{\bar{\rho} \in R(N, p)} \mathcal{F}_{\bar{\rho}},$$

such that $A_{\bar{\rho}} M_{\bar{\rho}} = M_{\bar{\rho}}$ and $A_{\bar{\rho}} M_{\bar{\rho}'} = 0$ if $\bar{\rho} \neq \bar{\rho}'$, and similarly for \mathcal{F} . In other words, $M_{\bar{\rho}}$ (or $\mathcal{F}_{\bar{\rho}}$) is the common generalized eigenspace in M (respectively \mathcal{F}) for all the operators T_ℓ and ℓS_ℓ ($\ell \nmid Np$) with generalized eigenvalues $\text{tr } \bar{\rho}(\text{Frob}_\ell)$ and $\det \bar{\rho}(\text{Frob}_\ell)$.

Let $\bar{\rho} \in R$. Since A acts faithfully on M , the algebra $A_{\bar{\rho}}$ acts faithfully on $M_{\bar{\rho}}$. In particular $M_{\bar{\rho}}$ is nonzero. It is easy to deduce that $M_{\bar{\rho}}$ contains a nonzero eigenform for all the Hecke operators T_ℓ and S_ℓ , $\ell \nmid Np$. We shall need on one occasion the following slightly more precise result, due to Ghitza [2006].

(3.15) Let $\bar{\rho} \in R$. There exists a form $f = \sum_{n=1}^\infty a_n q^n$ in $M_{\bar{\rho}}$, with $a_0 = 0$, $a_1 = 1$, that is an eigenform for all the Hecke operators T_ℓ and S_ℓ , $\ell \nmid Np$.

Indeed, according to [Ghitza 2006, Theorem 1], there exists an eigenform $h \in M_{\bar{\rho}}$ which is cuspidal, that is, such that $a_0(h) = 0$. Let $m \in \mathbb{N}$ with $a_m(h) \neq 0$. Then $f = (1/a_m(h))U_m h$ is an eigenform and satisfies $a_0(f) = 0$, $a_1(f) = 1$.

3G. The Hecke modules Af and the Hecke algebra A_f . For $f \in M(N, \mathbb{F})$, recall that we defined Af to be the submodule of M (over A) generated by f , which by (3.10) is a finite-dimensional vector space over \mathbb{F} . We shall denote by A_f the image of A under the restriction map $\text{End}_{\mathbb{F}}(M) \rightarrow \text{End}_{\mathbb{F}}(Af)$. Thus A_f is a finite-dimensional quotient of A . We continue to denote by T_ℓ and S_ℓ the images of T_ℓ and S_ℓ in A_f .

3H. The support $R(f)$ of a modular form. For $f \in M$, we define the support of f to be the subset of R consisting of those representations $\bar{\rho}$ such that the component $f_{\bar{\rho}}$ of f in $M_{\bar{\rho}}$ is nonzero. We will denote the support of f by $R(f)$. Thus $R(f) = \emptyset$ if and only if $f = 0$, and $R(f)$ is a singleton $\{\bar{\rho}\}$ if and only if f is a generalized eigenform for all the operators T_ℓ and S_ℓ (with $\ell \nmid Np$). Equivalently, $R(f)$ is the smallest subset of R such that the natural surjection $A = \prod_{\bar{\rho} \in R} A_{\bar{\rho}} \rightarrow A_f$ factors through $\prod_{\bar{\rho} \in R(f)} A_{\bar{\rho}}$. In view of (3.14), we have the following lemma.

Lemma 9. *Let $\ell \nmid Np$. The action of the operator T_ℓ on the finite-dimensional space Af is nilpotent if and only if $\text{Frob}_\ell \in N_{\bar{\rho}}$ for every $\bar{\rho} \in R(f)$. Similarly, the action of R_ℓ on Af is invertible if and only if $\text{Frob}_\ell \in U_{\bar{\rho}}$ for every $\bar{\rho} \in R(f)$.*

3I. Pure modular forms and the invariants $\alpha(f)$ and $h(f)$.

Definition 10. We say that $f \in M$ is *pure* if, for every $\bar{\rho}, \bar{\rho}' \in R(f)$, one has $N_{\bar{\rho}} = N_{\bar{\rho}'}$, or equivalently $U_{\bar{\rho}} = U_{\bar{\rho}'}$. If f is pure and nonzero, we denote by N_f and U_f the common sets $N_{\bar{\rho}}$ and $U_{\bar{\rho}}$ for $\bar{\rho} \in R(f)$. Further, we let \mathcal{N}_f and \mathcal{U}_f denote the sets of primes $\ell \nmid Np$ with $\text{Frob}_\ell \in N_f$ and $\text{Frob}_\ell \in U_f$ respectively.

Note that generalized eigenforms are pure, but that the converse is false in general. Also note that, by Lemma 9, if f is nonzero and pure and $\ell \nmid Np$, then T_ℓ is nilpotent on Af if $\ell \in \mathcal{N}_f$, and T_ℓ is invertible on Af if $\ell \in \mathcal{U}_f$.

Definition 11. Let f be a pure, nonzero, modular form. Define $\alpha(f) = \mu_{G_{\mathbb{Q}, Np}}(N_f)$ such that $\alpha(f) = \alpha(\bar{\rho})$ for any $\bar{\rho} \in R(f)$. Define the *strict order of nilpotence* of f , denoted by $h(f)$, as the largest integer h such that there exist (not necessarily distinct) prime numbers $\ell_1, \dots, \ell_h \nmid Np$ in \mathcal{N}_f with $T_{\ell_1} \cdots T_{\ell_h} f \neq 0$.

Note that, in the definition of the strict order of nilpotence, the largest integer h exists and is no more than the dimension of Af , since the T_{ℓ_i} act nilpotently on Af for $\ell_i \in \mathcal{N}_f$.

(3.16) Given a general nonzero form f , partition the finite set $R(f)$ into equivalence classes $R_i(f)$ based on the equivalence relation $\bar{\rho} \sim \bar{\rho}'$ if and only if $N_{\bar{\rho}} = N_{\bar{\rho}'}$. Thus we may write

$$f = \sum_i f_i, \quad f_i = \sum_{\bar{\rho} \in R_i(f)} f_{\bar{\rho}},$$

so that the f_i are pure. We call this decomposition the *canonical decomposition of f into pure forms*.

We now extend the definitions of $\alpha(f)$ and $h(f)$ to forms that are not necessarily pure.

Definition 12. If $f = \sum_i f_i$ is the canonical decomposition of f into pure forms, we set $\alpha(f) = \min_i \alpha(f_i)$ and $h(f) = \max_{i, \alpha(f_i) = \alpha(f)} h(f_i)$.

3J. Existence of a pseudorepresentation and consequences.

Proposition 13. *There exist continuous maps $t : G_{\mathbb{Q}, Np} \rightarrow A$ and $d : G_{\mathbb{Q}, Np} \rightarrow A$ such that*

- (i) d is a morphism of groups $G_{\mathbb{Q}, Np} \rightarrow A^*$,
- (ii) t is central (i.e., $t(gh) = t(hg)$),
- (iii) $t(1) = 2$,

- (iv) $t(gh) + t(gh^{-1})d(h) = t(g)t(h)$ for all $g, h \in G_{\mathbb{Q}, Np}$,
- (v) $t(\text{Frob}_\ell) = T_\ell$ for all $\ell \nmid Np$,
- (vi) $d(\text{Frob}_\ell) = \ell S_\ell$ for all $\ell \nmid Np$.

The uniqueness of such a pair (t, d) is clear: the function t is characterized uniquely by (ii) and (v) alone using the Chebotarev density theorem, and d is characterized by (i) and (vi) (or else by (iv); see (5) below). The existence of t and d is proved by “glueing” the traces and determinants of the representations attached by Deligne to eigenforms in characteristic zero and then reducing modulo p . For details, see [Bellaïche and Khare 2015].

Remark 14. The properties (i) to (iv) express the fact that (t, d) is a pseudorepresentation of dimension 2. The map t is called the trace, and the map d is called the determinant of the representation (t, d) (see [Chenevier 2014]). It is easy to check that the trace and determinant of any continuous two-dimensional representation (of a topological group over any topological commutative ring) satisfy properties (i) to (iv). Since $p > 2$, one can recover d from t by the formula

$$d(g) = (t(g)^2 - t(g^2))/2, \tag{5}$$

which follows upon taking $g = h$ in (iv) and using (iii).

We prove for later use the following lemma.

Lemma 15. *For every $g \in G_{\mathbb{Q}, Np}$ one has $t(g^p) = t(g)^p$.*

Proof. Let $m \in \text{GL}_2(A)$ be the matrix $\begin{pmatrix} 0 & -1 \\ d(g) & t(g) \end{pmatrix}$ with $\text{tr}(m) = t(g)$ and $\det(m) = d(g)$. Since tr and \det on the multiplicative subgroup generated by m satisfy properties (i) to (iv) above, one sees easily by induction on n that $\text{tr}(m^n) = t(g^n)$ for all n . Thus it suffices to prove that $\text{tr}(m^p) = \text{tr}(m)^p$.

Let $f : \mathbb{F}_p[D, T] \rightarrow A$ be the morphism of rings sending D to $d(g)$ and T to $t(g)$, where D and T are two indeterminates. Let $M \in \text{GL}_2(\mathbb{F}_p[D, T])$ be the matrix $\begin{pmatrix} 0 & -1 \\ D & T \end{pmatrix}$. Since $f(M) = m$, it clearly suffices to prove that $\text{tr}(M^p) = \text{tr}(M)^p$. Since $\mathbb{F}_p[D, T]$ can be embedded in an algebraic field k of characteristic p , it suffices to prove that, for all $M \in M_2(k)$, one has $\text{tr}(M^p) = \text{tr}(M)^p$. Replacing M by a conjugate matrix if necessary, we may assume that M is triangular, in which case the formula is obvious. □

Let $f \in M(N, \mathbb{F})$ be a modular form. Let $t_f : G \rightarrow A_f$ and $d_f : G \rightarrow A_f$ be the composition of t and d with the natural morphism of algebras $A \rightarrow A_f$. Note that (t_f, d_f) satisfies the same properties (i) to (vi), and so (t_f, d_f) is a pseudorepresentation of G on A_f . In particular, (v) reads

$$t_f(\text{Frob}_\ell)f = T_\ell f. \tag{6}$$

We now deduce certain consequences of the existence of the pseudorepresentation (t, d) for the algebra A and for modular forms $f \in M$.

Proposition 16. *The Hecke algebra A is topologically generated by the T_ℓ for $\ell \nmid Np$ alone (that is, without the S_ℓ).*

Proof. Let A' be the closed subalgebra of A generated by the T_ℓ . Since the elements Frob_ℓ for $\ell \nmid Np$ are dense in $G_{\mathbb{Q}, Np}$ and $t(\text{Frob}_\ell) = T_\ell \in A'$, one sees that $t(G_{\mathbb{Q}, Np}) \subset A'$. In particular, for ℓ not dividing Np , we have $t(\text{Frob}_\ell^2) \in A'$, hence we also have $(t(\text{Frob}_\ell^2) - t(\text{Frob}_\ell)^2)/2$. But this element is just $d(\text{Frob}_\ell) = \ell S_\ell$. Hence $S_\ell \in A'$ and $A' = A$. \square

Lemma 17. *There exists a finite quotient G_f of $G_{\mathbb{Q}, Np}$ such that, for $\ell \nmid Np$, the action of T_ℓ on A_f depends only on the image of Frob_ℓ in G_f .*

Proof. Let H denote the subset of $G_{\mathbb{Q}, Np}$ consisting of elements h such that $t_f(gh) = t_f(g)$ for every $g \in G$. Since t is central (property (ii) above), it follows that H is a normal subgroup of G . We call H the *kernel* of the pseudorepresentation (t_f, d_f) . By (5) and (iii) one has $d_f(h) = 1$ for $h \in H$. Let $G_f = G_{\mathbb{Q}, Np}/H$. The maps $t_f, d_f : G_{\mathbb{Q}, Np} \rightarrow A_f$ factor through G_f to give maps $G_f \rightarrow A_f$, which we shall also denote by t_f and d_f . Note that, by construction, there is no $h \neq 1$ in G_f such that $t_f(gh) = t_f(g)$ for every $g \in G_f$. Since A_f is finite, it follows easily that G_f is a finite group. Finally, by (6), $T_\ell f$ depends only on $t_f(\text{Frob}_\ell)$, which only depends on the image of Frob_ℓ in G_f . Therefore, if $g \in A_f$, then $g = Tf$ for some $T \in A$, and $T_\ell g = T_\ell Tf = TT_\ell f$ depends only on the image of Frob_ℓ in G_f . \square

We draw three consequences of this lemma.

Proposition 18. *Let $f = \sum_{n=0}^\infty a_n q^n \in \mathcal{F} = \mathcal{F}(N, \mathbb{F})$. If $f \neq 0$, then there exists a square-free integer n such that $a_n \neq 0$.*

Proof. Since f is nonzero, $a_n \neq 0$ for some $n \in \mathbb{N}$, and since $f \in \mathcal{F}$, one has $(n, Np) = 1$. Thus $a_1(T_n f) \neq 0$. By Proposition 16, T_n is a limit of linear combinations of terms of the form $T_{\ell_1} \cdots T_{\ell_s}$ with ℓ_1, \dots, ℓ_s being (not necessarily distinct) primes all not dividing Np . Since $T \mapsto a_1(Tf)$ is continuous and linear, we deduce that $a_1(T_{\ell_1} \cdots T_{\ell_s} f) \neq 0$ for some primes ℓ_1, \dots, ℓ_s not dividing Np (again not necessarily distinct). Since the action of T_{ℓ_i} on A_f depends only on Frob_{ℓ_i} in the finite Galois group G_f , one can replace ℓ_i by any other prime whose Frobenius has the same image without affecting the action of T_{ℓ_i} . In this manner, we may find distinct primes ℓ'_i such that $T_{\ell_1} \cdots T_{\ell_s} = T_{\ell'_1} \cdots T_{\ell'_s}$, and then with $m = \ell'_1 \cdots \ell'_s$ it follows that $a_m(f) = a_1(T_m f) = a_1(T_{\ell'_1} \cdots T_{\ell'_s} f) = a_1(T_{\ell_1} \cdots T_{\ell_s} f) \neq 0$. \square

Proposition 19. *Let $f \in M(N, \mathbb{F})$ be a pure form, and let f' be any element of $M(N, \mathbb{F})$. Let h be a nonnegative integer, and let \mathcal{M} denote the set of square-free integers m having exactly h prime factors, all from the set \mathcal{N}_f , and such that $T_m f = f'$. Then \mathcal{M} is multifrobenian.*

Proof. Let G_f be as in Lemma 17 and let $D_{f,f'} \subset G_f^h$ denote the set of h -tuples (g_1, \dots, g_h) such that $t_f(g_1) \cdots t_f(g_h)f = f'$, where $g_i \in \mathcal{N}_f$ for $i = 1, \dots, h$. Then $D_{f,f'}$ is invariant under conjugation and symmetric under permutations, and hence by definition \mathcal{M} is the multifrobenian set of weight h attached to $D_{f,f'}$ and G_f . \square

Proposition 20. *Let f be a pure modular form. Then there exist $h(f)$ distinct primes $\ell_1, \dots, \ell_{h(f)}$ in \mathcal{N}_f such that $T_{\ell_1} \cdots T_{\ell_{h(f)}}f \neq 0$.*

Proof. The fact that we can find $h(f)$ primes $\ell_1, \dots, \ell_{h(f)}$ in \mathcal{N}_f such that $f' := T_{\ell_1} \cdots T_{\ell_{h(f)}}f \neq 0$ simply follows from the definition of $h(f)$. In the notation of the previous proposition we see that $D_{f,f'}$ is not empty as it contains $(\text{Frob}_{\ell_1}, \dots, \text{Frob}_{\ell_{h(f)}})$. Hence the multifrobenian set \mathcal{M} of that proposition is not empty, and there exist distinct primes $\ell'_1, \dots, \ell'_{h(f)}$ in \mathcal{N}_f such that $T_{\ell'_1} \cdots T_{\ell'_{h(f)}}f = f' \neq 0$. \square

4. Asymptotics: proof of Theorem 1

Let $f = \sum a_n q^n \in M = M(N, \mathbb{F})$. We assume below that f is not constant. We set

$$Z(f) = \{n \in \mathbb{N}, a_n \neq 0\} \quad \text{and} \quad \pi(f, x) = |\{n < x, a_n \neq 0\}|,$$

and our goal is to establish an asymptotic formula for $\pi(f, x)$. For a given $a \in \mathbb{F}^*$ it will also be convenient to define

$$Z(f, a) = \{n \in \mathbb{N}, a_n = a\} \quad \text{and} \quad \pi(f, a, x) = |\{n < x, a_n = a\}|.$$

By (3.8), we may assume without loss of generality that $(N, p) = 1$, so all the results of Section 3 apply.

4A. Proof of Theorem 1 when $f \in \mathcal{F}(N, \mathbb{F})$ and f is pure. We assume in this section that f is a pure form in $\mathcal{F}(N, \mathbb{F})$. From Section 3I recall that the set of primes ℓ not dividing Np may be partitioned into two sets, \mathcal{U}_f and \mathcal{N}_f , such that $\ell \in \mathcal{U}_f$ if T_ℓ acts invertibly on Af and $\ell \in \mathcal{N}_f$ if T_ℓ acts nilpotently on Af .

Given $a \in \mathbb{F}^*$ we wish to prove an asymptotic formula for $\pi(f, a, x)$. If n is an integer with $a_n(f) = a$ (and since $f \in \mathcal{F}$ we must have $(n, Np) = 1$) then we may write $n = mm'm''$ with m square-free and containing all prime factors from \mathcal{U}_f , with m' square-free and containing $h \leq h(f)$ prime factors all from \mathcal{N}_f , and with m'' square-full and coprime to mm' . Such a decomposition of the number n is unique, and if we write $f'' = T_{m''}f$ and $f' = T_{m'}f''$ then f' and f'' are forms in $Af - \{0\}$ with $a_m(f') = a$. Thus integers n with $a_n(f) = a$ uniquely define triples (f', f'', h) and we may decompose

$$Z(f, a) = \coprod_{f', f'', h} Z(f, a; f', f'', h), \tag{7}$$

where the disjoint union is taken over forms f', f'' in $Af - \{0\}$ and integers $0 \leq h \leq h(f)$. Here the set $Z(f, a; f', f'', h)$ is defined as the set of integers $n = mm'm''$ with $(n, Np) = 1$ such that

- (4.1) m is square-free and all its prime factors are in \mathcal{U}_f ;
- (4.2) m' is square-free, has exactly h prime factors, and all its prime factors are in \mathcal{N}_f , and moreover $f' = T_{m'}f''$;
- (4.3) m'' is square-full, relatively prime to mm' , and $f'' = T_{m''}f$;
- (4.4) $a_m(f') = a$.

Next we evaluate the number of elements up to x in the set $Z(f, a; f', f'', h)$ using Theorem 7. Write $\mathcal{S}_{f,f''}$ for the set of square-full integers m'' such that $T_{m''}f = f''$, and write $\mathcal{M}_{f',f''}$ for the set of integers m' that are the product of h distinct primes in \mathcal{N}_f and such that $f' = T_{m'}f''$. By Proposition 19, $\mathcal{M}_{f',f''}$ is a multifrobenian set of height h . Observe that conditions (4.1), (4.2), (4.3) are the same as conditions (2.1.1), (2.1.2), (2.1.3) defining the set $\mathcal{Z}(\mathcal{U}_f, \mathcal{M}_{f',f''}, \mathcal{S}_{f,f''})$. Now, define a map $\tau_f : \mathcal{U}_f \rightarrow A_f^*$ sending ℓ to $t_f(\text{Frob}_\ell) = T_\ell$ and extend it by multiplicativity to the set of all square-free integers composed only of primes from \mathcal{U}_f . Let Γ_f be the image of τ_f , which is a finite abelian subgroup of the finite group A_f^* , and let $\Delta_{f',a}$ denote the set of $\gamma \in \Gamma_f$ such that $a_1(\gamma f') = a$. For $n = mm'm'' \in Z(f, a; f', f'', h)$ set $\tau_f(n) = \tau_f(m)$ so that condition (4.4) is the same as $\tau_f(n) \in \Delta_{f',a}$. Thus we are in a position to apply Theorem 7, which yields, assuming that the sets $\mathcal{M}_{f',f''}, \mathcal{S}_{f,f''}$ and $\Delta_{f',a}$ are all not empty,

$$\begin{aligned}
 & |\{n < x : n \in Z(f, a; f', f'', h)\}| \\
 &= |\{n < x : n \in \mathcal{Z}(\mathcal{U}_f, \mathcal{M}_{f',f''}, \mathcal{S}_{f,f''}), \tau(n) \in \Delta_{f',a}\}| \\
 &\sim c \delta(\mathcal{M}_{f',f''}) \frac{|\Delta_{f',a}|}{|\Gamma_f|} \frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^h, \tag{8}
 \end{aligned}$$

where $c = c(f, f'') > 0$ is a constant depending only on \mathcal{U}_f and $\mathcal{S}_{f,f''}$ (thus only on f and f''), and $\alpha(f) = 1 - \delta(\mathcal{U}_f) = \delta(\mathcal{N}_f)$ as defined in Section 3I. If at least one of the sets $\mathcal{M}_{f',f''}, \mathcal{S}_{f,f''}$ or $\Delta_{f',a}$ is empty, then so is $Z(f, a; f', f'', h)$.

Using (7), one deduces that either all the $Z(f, a, f', f'', h)$ are empty for all permissible choices of (f', f'', h) , in which case $\pi(f, a, x) = 0$ for all x , or

$$\pi(f, a, x) \sim c(f, a) \frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f,a)}, \tag{9}$$

where $h(f, a) \leq h(f)$ is the largest integer $h \leq h(f)$ for which there exist forms $f', f'' \in Af - \{0\}$ such that $Z(f, a; f', f'', h)$ is not empty, and where

$$c(f, a) = \sum_{(f', f'', h(f,a))} c(f, f'') \delta(\mathcal{M}_{f',f''}) \frac{\#\Delta_{f',a}}{\#\Gamma_f}, \tag{10}$$

the sum being over those $f', f'' \in Af - \{0\}$ such that $Z(f, a; f', f'', h(f, a))$ is not empty.

We claim that the set $Z(f, a; f', f'', h(f))$ is not empty for some choice of $(f', f'') \in (Af - \{0\})^2$ and some $a \in \mathbb{F}^*$. To see this, take $m'' = 1$ and $f'' = f = T_{m''} f$. By Proposition 20, there exists an integer m' with $h(f)$ distinct prime factors in \mathcal{N}_f such that $T_{m'} f \neq 0$. Fix one such m' and let $f' = T_{m'} f$. Proposition 18 tells us that there exists a square-free integer m such that $a_m(f') \neq 0$. Note that $h(f') = 0$, hence m has all its prime factors in \mathcal{U}_f . Define $a = a_m(f') \in \mathbb{F}^*$. Then the set $Z(f, a; f', f'', h(f))$ contains $n = mm'm''$ and is therefore not empty, which proves the claim.

Since $\pi(f, x) = \sum_{a \in \mathbb{F}^*} \pi(f, a, x)$, it follows from (9) and the above claim that

$$\pi(f, x) \sim c(f) \frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f)}, \quad \text{with } c(f) = \sum_{\substack{a \in \mathbb{F}^* \\ h(f,a)=h(f)}} c(f, a). \quad \square$$

4B. Proof of Theorem 1 when $f \in \mathcal{F}(N, \mathbb{F})$ but f is not necessarily pure. Let $f = \sum_i f_i$ be the canonical decomposition (see (3.16)) of f into pure forms. By the preceding section, one has

$$\pi(f_i, x) \sim c(f_i) \frac{x}{(\log x)^{\alpha(f_i)}} (\log \log x)^{h(f_i)}.$$

Consider the indices i such that $\alpha(f_i)$ is minimal (and by definition $\alpha(f_i) = \alpha(f)$); among those, select the indices with $h(f_i)$ maximal (and by definition $h(f_i) = h(f)$). Let I denote the set of such indices. We claim that

$$\pi(f, x) \sim c(f) \frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f)}, \quad \text{with } c(f) = \sum_{i \in I} c(f_i).$$

To prove the claim, first note that we can forget those f_i with $i \notin I$, because they have a negligible contribution compared to the asserted asymptotics (either the power of $\log \log x$ is smaller, or the power of $\log x$ is larger). It remains to prove that, for $i, j \in I, i \neq j$, one has

$$\pi(f_i, f_j, x) = o\left(\frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f)}\right), \tag{11}$$

where $\pi(f_i, f_j, x) = |\{n \leq x, a_n(f_i) \neq 0, a_n(f_j) \neq 0\}|$. But if n is such that $a_n(f_i) \neq 0$ and $a_n(f_j) \neq 0$, it has at most $h(f_i) + h(f_j) = 2h(f)$ prime factors ℓ such that $\text{Frob}_\ell \in N_{f_i} \cup N_{f_j}$. Moreover, the two open sets N_{f_i} and N_{f_j} of $G_{\mathbb{Q}, Np}$ are not equal by definition of the decomposition into pure forms (3.16). Therefore the measure α' of the open set $N_{f_i} \cup N_{f_j}$ is strictly greater than the common measure

$\alpha(f) = \alpha(f_i) = \alpha(f_j)$ of N_{f_i} and N_{f_j} . Hence an application of Theorem 7 gives

$$\pi(f_1, f_j, x) = O\left(\frac{x}{(\log x)^{\alpha'}} (\log \log x)^{2h(f)}\right),$$

which implies (11) since $\alpha' > \alpha(f)$. □

4C. Proof of Theorem 1: general case. Let \mathcal{B} be the set of integers $m \geq 1$ all of whose prime factors divide Np . Note that the series $\sum_{m \in \mathcal{B}} 1/m$ converges. For $m \in \mathcal{B}$, we consider the following operators on $\mathbb{F}[[q]]$:

$$U_m\left(\sum a_n q^n\right) = \sum a_{mn} q^n \quad \text{and} \quad V_m\left(\sum a_n q^n\right) = \sum a_n q^{mn}.$$

We also consider the operator W defined by

$$W\left(\sum a_n q^n\right) = \sum_{(n, Np)=1} a_n q^n.$$

The operators U_m stabilize the space $M(N, \mathbb{F})$ (see Section 3C). The operator V_m however does not stabilize $M(N, \mathbb{F})$ (except for $m = p$; see (3.11)), but it sends $M(N, \mathbb{F})$ into $M(Nm, \mathbb{F})$ since it is the reduction modulo p of the action on q -expansions of the operator on modular forms $f(z) \mapsto f(mz)$. As for the operator W , it is easily seen from the definitions to satisfy

$$W = \sum_{m \in \mathcal{B}} \mu(m) V_m U_m,$$

where $\mu(m)$ is the Möbius function. Since μ vanishes on integers that are not square-free, the sum is in fact finite, and it follows that W sends $M(N, \mathbb{F})$ into $M(N^2, \mathbb{F})$ and, more precisely, into $\mathcal{F}(N^2, \mathbb{F})$.

Let $f = \sum a_n q^n \in M(N, \mathbb{F})$ be a modular form. For any integer $m \in \mathcal{B}$, define

$$f_m = \sum_{\substack{n=mm' \\ (m', Np)=1}} a_n q^n,$$

so that $f = a_0 + \sum_{m \in \mathcal{B}} f_m$. This sum may genuinely be infinite, but it obviously converges in $\mathbb{F}[[q]]$. Clearly

$$\pi(f, x) = \sum_{m \in \mathcal{B}} \pi(f_m, x) + O(1),$$

where the error term $O(1)$ is just 0 if $a_0 = 0$ and 1 otherwise. One sees from the definitions that $f_m = V_m W U_m f$, so that

$$\pi(f_m, x) = \pi(W U_m f, x/m).$$

Since $\pi(f_m, x)$ is clearly at most x/m , and since $\sum_{m \in \mathcal{B}, m > (\log x)^2} 1/m \ll 1/\log x$, we conclude that

$$\pi(f, x) = \sum_{\substack{m \in \mathcal{B} \\ m \leq (\log x)^2}} \pi(WU_m f, x/m) + O\left(\frac{x}{\log x}\right). \tag{12}$$

Now $WU_m f \in \mathcal{F}(N^2, \mathbb{F})$, and we can apply the results of Section 4B and thus estimate $\pi(WU_m f, x/m)$. Thus, if $WU_m f \neq 0$ and $m \leq (\log x)^2$ (so that $\log(x/m) \sim \log x$), then

$$\pi(WU_m f, x/m) \sim c(WU_m f) \frac{x}{m(\log x)^{\alpha(WU_m f)}} (\log \log x)^{h(WU_m f)}. \tag{13}$$

Note that, since f is not a constant, $WU_m f \neq 0$ for at least one $m \in \mathcal{B}$. Further, note that, while \mathcal{B} is infinite, the set of forms $WU_m f$ for $m \in \mathcal{B}$ is finite since $U_m f$ belongs to the Hecke-module generated by f which is finite-dimensional over \mathbb{F} (see (3.10)). Thus the asymptotic formula (13) holds uniformly for all $m \leq (\log x)^2$ with $m \in \mathcal{B}$ and as $x \rightarrow \infty$. Finally, since the Hecke operators T_ℓ for ℓ prime to Np commute with the operators U_m, V_m and W , it follows that

$$\alpha(f) = \min_{\substack{m \in \mathcal{B} \\ WU_m f \neq 0}} \alpha(WU_m f) \quad \text{and} \quad h(f) = \max_{\substack{m \in \mathcal{B} \\ WU_m f \neq 0 \\ \alpha(WU_m f) = \alpha(f)}} h(WU_m f).$$

Thus, setting $c_m = c(WU_m f)$ when $WU_m f \neq 0$ (which happens for at least one $m \in \mathcal{B}$) and setting $c_m = 0$ otherwise, we may recast (13) as

$$\pi(WU_m f, x/m) = (c_m + \epsilon_m(x)) \frac{x}{m(\log x)^{\alpha(f)}} (\log \log x)^{h(f)}, \tag{14}$$

where $\epsilon_m(x) \rightarrow 0$ as $x \rightarrow \infty$, uniformly for all $m \in \mathcal{B}$ with $m \leq (\log x)^2$.

From (12) and (14) we obtain

$$\pi(f, x) \sim \sum_{\substack{m \in \mathcal{B} \\ m < (\log x)^2}} \frac{c_m}{m} \frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f)} \sim c \frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f)},$$

with

$$c = \sum_{m \in \mathcal{B}} \frac{c_m}{m}, \tag{15}$$

noting that this series converges because c_m takes only finitely many values (and hence is bounded). This finishes the proof of Theorem 1. □

5. Equidistribution

Definition 21. We say that a form $f \in M(\Gamma_1(N), \mathbb{F})$ has the *equidistribution property* if, for any two $a, b \in \mathbb{F}^*$, we have $\pi(f, a, x) \sim \pi(f, b, x)$. We say that a

subspace $V \subset M(\Gamma_1(N), \mathbb{F})$ has the *equidistribution property* if every nonconstant form $f \in V$ has the equidistribution property.

In view of Theorem 1, f having the equidistribution property is equivalent to

$$\pi(f, a, x) \sim \frac{c(f)}{|\mathbb{F}| - 1} \frac{x}{\log(x)^{\alpha(f)}} (\log \log x)^{h(f)},$$

where $c(f)$ is the constant of Theorem 1.

We now give a sufficient condition for equidistribution for generalized eigenforms, which generalizes a similar criterion for true eigenforms due to Serre [1976, Exercise 6.10].

Proposition 22. *Let $\bar{\rho} : G_{\mathbb{Q}, Np} \rightarrow \mathrm{GL}_2(\mathbb{F})$ be a representation in $R(N, p)$. If the set $\mathrm{tr} \bar{\rho}(G_{\mathbb{Q}, Np}) - \{0\}$ generates \mathbb{F}^* multiplicatively, then the generalized eigenspace $M(N, \mathbb{F})_{\bar{\rho}}$ has the equidistribution property.*

Proof. First assume that $f \in \mathcal{F}(N, \mathbb{F})_{\bar{\rho}}$. Since f is pure, the asymptotic formula (9) holds for $\pi(f, a, x)$, and to obtain equidistribution it remains to show that the constant $c(f, a)$ appearing there is independent of $a \in \mathbb{F}^*$. By formula (10), which gives the values of $c(f, a)$, it suffices to prove that the cardinalities of the subsets $\Delta_{f', a}$ of Γ_f are independent of $a \in \mathbb{F}^*$, for any given form $f' \in Af - \{0\}$. Recall that Γ_f is the subgroup of A_f^* generated by the elements $T_\ell = t_f(\mathrm{Frob}_\ell)$ for $\ell \in \mathcal{U}_f = \mathcal{U}_{\bar{\rho}}$ and hence, by Chebotarev and the definition of \mathcal{U}_f , the subgroup of A_f^* generated by $t_f(G_{\mathbb{Q}, Np}) \cap A_f^*$. Recall also that $\Delta_{f', a}$ is the set of elements $\gamma \in \Gamma_f$ such that $a_1(\gamma f') = a$. To prove that $|\Delta_{f', a}|$ is independent of a , it therefore suffices to prove that Γ_f contains the subgroup \mathbb{F}^* of A_f^* , in which case multiplication by ba^{-1} will induce a bijection between $\Delta_{f', a}$ and $\Delta_{f', b}$ for any $b \in \mathbb{F}^*$. Since by hypothesis $\mathrm{tr} \bar{\rho}(G_{\mathbb{Q}, Np}) - \{0\}$ generates \mathbb{F}^* , it suffices to show that $\mathrm{tr} \bar{\rho}(G_{\mathbb{Q}, Np}) - \{0\} \subset \Gamma_f$. For this, let $g \in G_{\mathbb{Q}, Np}$, and assume that $\mathrm{tr} \bar{\rho}(g) \neq 0$. By (3.14), one has $t_f(g) \equiv \mathrm{tr} \bar{\rho}(g) \pmod{\mathfrak{m}_{A_f}}$ where \mathfrak{m}_{A_f} is the maximal ideal of the finite local algebra A_f . Let n be an integer such that $\mathfrak{m}_{A_f}^n = 0$, and let q be the cardinality of \mathbb{F} . Then, by Lemma 15,

$$t_f(g^{q^n}) = t_f(g)^{q^n} \equiv (\mathrm{tr} \bar{\rho}(g))^{q^n} \pmod{\mathfrak{m}_{A_f}^n},$$

so that, since $x \mapsto x^q$ induces the identity on \mathbb{F} ,

$$t_f(g^{q^n}) = \mathrm{tr} \bar{\rho}(g).$$

Hence $\mathrm{tr} \bar{\rho}(g) \in \Gamma_f$ and this completes the proof of the proposition for forms $f \in \mathcal{F}(N, \mathbb{F})_{\bar{\rho}}$.

Now consider a general nonconstant form $f \in \mathcal{M}(N, \mathbb{F}_{\bar{p}})$. Mimicking the proof in Section 4C, one has

$$\pi(f, a, x) = \sum_{\substack{m \in \mathcal{B} \\ m \leq (\log x)^2}} \pi(WU_m f, a, x/m) + O\left(\frac{x}{\log x}\right)$$

and the asymptotic formula obtained for $\pi(WU_m f, a, x/m)$ is independent of $a \in \mathbb{F}^*$, since $WU_m f \in \mathcal{F}(N^2, \mathbb{F}_{\bar{p}})$ and by the result just established. □

Serre has given an example of an eigenform $f \pmod p$ that does not have the equidistribution property: namely, the form $\Delta \pmod 7$ (see [Serre 1976, Exercise 12]). Here is a generalization.

Proposition 23. *Suppose f is a nonconstant eigenform in $\mathcal{F}(N, \mathbb{F}_{\bar{p}})$. If the set $\text{tr } \bar{\rho}(G_{\mathbb{Q}, Np}) - \{0\}$ does not generate \mathbb{F}^* multiplicatively, then f does not have the equidistribution property.*

Proof. Let $f = \sum_{n=1}^{\infty} a_n q^n$. Since f is an eigenform for the T_ℓ , $\ell \nmid Np$, and also is killed by the U_ℓ for $\ell \mid Np$ (because it is in \mathcal{F}), the sequence a_n is multiplicative and one has $a_\ell = 0$ for $\ell \mid Np$ and $a_\ell = \text{tr } \bar{\rho}(\text{Frob}_\ell)$ for all $\ell \nmid Np$. Also one has $a_1 \neq 0$ since f is nonconstant, and we may assume $a_1 = 1$.

Let B be the proper subgroup of \mathbb{F}^* generated by $\text{tr } \bar{\rho}(G_{\mathbb{Q}, Np}) - \{0\}$. By multiplicativity, $a_n \in B \cup \{0\}$ for all square-free integers m . Since $a_n \neq 0$ for square-free n exactly when n is composed only of primes in \mathcal{U}_f , we see that

$$\sum_{\substack{n \leq x \\ a_n \in B}} 1 \geq \sum_{\substack{n \leq x \\ n \text{ square-free} \\ p \mid n \Rightarrow p \in \mathcal{U}_f}} 1 \sim c \frac{x}{(\log x)^{\alpha(f)}} \tag{16}$$

for a suitable positive constant c . Now if f has the equidistribution property, then, since $|B| \leq |\mathbb{F}^* - B|$ for proper subgroups B of \mathbb{F}^* , we must have

$$\sum_{\substack{n \leq x \\ a_n \in B}} 1 \leq (1 + o(1)) \sum_{\substack{n \leq x \\ a_n \in \mathbb{F}^* - B}} 1.$$

The right-hand side above is at most the number of integers of the form $mr \leq x$ where $1 < m$ is square-full and $r \leq x/m$ is square-free with $(r, m) = 1$ and $a_r \neq 0$. Ignoring the condition $(r, m) = 1$, the number of such integers is (arguing as in Section 4C)

$$\leq \sum_{\substack{1 < m \leq x \\ m \text{ square-full}}} \sum_{\substack{r \leq x/m \\ r \text{ square-free} \\ p \mid r \Rightarrow p \in \mathcal{U}_f}} 1 \leq \sum_{\substack{1 < m \leq (\log x)^2 \\ m \text{ square-full}}} \frac{x}{m} \frac{c + o(1)}{(\log x)^{\alpha(f)}} + \sum_{\substack{m > (\log x)^2 \\ m \text{ square-full}}} \frac{x}{m},$$

which is at most

$$\begin{aligned} (c + o(1)) \frac{x}{(\log x)^{\alpha(f)}} \sum_{\substack{1 < m \\ m \text{ square-full}}} \frac{1}{m} &= (c + o(1)) \frac{x}{(\log x)^{\alpha(f)}} \left(\frac{\zeta(2)\zeta(3)}{\zeta(6)} - 1 \right) \\ &= ((0.9435 \dots)c + o(1)) \frac{x}{(\log x)^{\alpha(f)}}. \end{aligned}$$

But this contradicts the lower bound (16), completing our proof. □

We can use the above result to give a converse to Proposition 22 when the level N is equal to 1.

Proposition 24. *Let $\bar{\rho} \in R(1, \mathbb{F})$. The space $M(1, \mathbb{F})_{\bar{\rho}}$ has the equidistribution property if and only if the set $\text{tr } \bar{\rho}(G_{\mathbb{Q}, p}) - \{0\}$ generates \mathbb{F}^* multiplicatively.*

Proof. By (3.15), $M(1, \mathbb{F})_{\bar{\rho}}$ has an eigenform $f = \sum_{n=1}^{\infty} a_n q^n$ with $a_1 = 1$ for all the Hecke operators T_ℓ and S_ℓ , $\ell \neq p$. Replacing f by $f - V_p U_p f$ (see (3.11)), we may assume that f is an eigenform in $\mathcal{F}(1, \mathbb{F})_{\bar{\rho}}$. If $M(1, \mathbb{F})_{\bar{\rho}}$, hence f , has the equidistribution property, then by the preceding proposition $\text{tr } \bar{\rho}(G_{\mathbb{Q}, p}) - \{0\}$ generates \mathbb{F}^* multiplicatively. □

In the same spirit, but concerning forms that are not necessarily generalized eigenforms, one has the following partial result.

Proposition 25. *If 2 is a primitive root modulo p , then $M(N, \mathbb{F}_p)$ has the equidistribution property.*

Proof. One reduces to the case of an $f \in \mathcal{F}(N, p)$ pure exactly as in Section 4B. Then, arguing as in the proof of Proposition 22, it suffices to prove that the group Γ_f generated by $t_f(G_{\mathbb{Q}, Np})$ contains \mathbb{F}_p^* . But Γ_f contains $t_f(1) = 2$ which by hypothesis generates \mathbb{F}_p^* . □

Again, one has a partial converse to this proposition.

Proposition 26. *In the case $N = 1$ and $p \equiv 3 \pmod{4}$, $M(1, \mathbb{F}_p)$ has the equidistribution property if and only if 2 is a primitive root modulo p .*

Proof. Let $\omega_p : G_{\mathbb{Q}, p} \rightarrow \mathbb{F}_p^*$ be the cyclotomic character modulo p , and define $\bar{\rho} = 1 \oplus \omega_p^{(p-1)/2}$. The hypothesis $p \equiv 3 \pmod{4}$ means that $(p - 1)/2$ is odd, and so $\bar{\rho}$ is odd and thus belongs to $R(1, p)$ ($\bar{\rho}$ is the representation attached to the Eisenstein series $E_k(z)$ where $k = 1 + (p - 1)/2$ for $p > 3$ and to $E_4(z)$ if $p = 3$). Reasoning as in Proposition 24, there is an eigenform f in $\mathcal{F}(1, p)_{\bar{\rho}}$. If $M(1, p)$, hence f , has the equidistribution property, then $\bar{\rho}(G_{\mathbb{Q}, p}) - \{0\}$ generates \mathbb{F}_p^* by Proposition 23. Since the image of $\bar{\rho}$ is $\{0, 2\}$, this implies that 2 is a primitive root modulo p . □

6. A variant: counting square-free integers with nonzero coefficients

Given a modular form $f = \sum_{n=0}^{\infty} a_n q^n$ in $M(N, p)$, let

$$\pi_{\text{sf}}(f, x) = |\{n < x, n \text{ square-free, } a_n \neq 0\}|.$$

Our proof of Theorem 1 allows us to get asymptotics for $\pi_{\text{sf}}(f, x)$, and indeed this is a little simpler than Theorem 1. We state this asymptotic result, and sketch the changes to our proof, omitting details.

Theorem 27. *If there exists a square-free integer n with $a_n \neq 0$, then there exists a positive real constant $c_{\text{sf}}(f) > 0$ such that*

$$\pi_{\text{sf}}(f, x) \sim c_{\text{sf}}(f) \frac{x}{(\log x)^{\alpha(f)}} (\log \log x)^{h(f)}.$$

If $a_n = 0$ for all square-free integers n , then in fact $a_n \neq 0$ only for those integers n that are divisible by ℓ^2 for some prime ℓ dividing Np .

Suppose below that f has some coefficient $a_n \neq 0$ with n not divisible by the square of any prime dividing Np . We first prove Theorem 27 for a pure form $f \in \mathcal{F}(N, p)$, as in Section 4A. In this case, our hypothesis on f is equivalent to saying that f is nonconstant. Then the proof given in Section 4A works by replacing the sets $Z(f), Z(f, a)$ by their intersection $Z_{\text{sf}}(f), Z_{\text{sf}}(f, a)$ with the set of square-free integers. We have a decomposition, analogous to (7) but simpler:

$$Z_{\text{sf}}(f, a) = \bigsqcup_{f', h} Z_{\text{sf}}(f, a; f', h), \tag{17}$$

where the disjoint union is taken over forms f' in $Af - \{0\}$ and over integers $0 \leq h \leq h(f)$. Here the set $Z_{\text{sf}}(f, a; f', h)$ is defined as the set of integers $n = mm'$ with $(n, Np) = 1$ such that

- (6.1) m is square-free and all its prime factors are in \mathcal{U}_f ;
- (6.2) m' is square-free, has exactly h prime factors, and all its prime factors are in \mathcal{N}_f , and moreover $f' = T_{m'} f$;
- (6.3) $a_m(f') = a$.

The asymptotics for the number of integers less than x in $Z(f, a; f', h)$ is then exactly as in Section 4A, except that the set of square-full integers $\mathcal{S}_{f, f''}$ is now $\{1\}$. The desired asymptotics for $\pi_{\text{sf}}(f)$ follows.

The case where f is in $\mathcal{F}(N, \mathbb{F})$ but not necessarily pure is reduced to the pure case exactly as in Section 4B.

Finally, in the general case where $f \in M(N, \mathbb{F})$, let \mathcal{B}_{sf} be the set of *square-free integers* m whose prime factors all divide Np . We observe that \mathcal{B}_{sf} is a finite subset

of the infinite set \mathcal{B} defined in Section 4C. For $m \in \mathcal{B}_{\text{sf}}$, we define as in Section 4C

$$f_m = \sum_{\substack{n=mm' \\ (m', Np)=1}} a_n q^n,$$

and we have clearly

$$\pi_{\text{sf}}(f, x) = \sum_{m \in \mathcal{B}_{\text{sf}}} \pi_{\text{sf}}(f_m, x).$$

By the assumption made on f , at least one of the f_m for $m \in \mathcal{B}_{\text{sf}}$ is nonconstant. The rest of the proof is therefore exactly as in Section 4C.

7. Examples

7A. Examples in the case $N = 1, p = 3$. The simplest case where our theory applies is $N = 1, p = 3$. Let us denote by $\Delta = q + 2q^4 + q^7 + q^{13} + \dots \in \mathbb{F}_3[[q]]$ the reduction modulo 3 of the q -expansion of the usual Δ function. The space $M(1, \mathbb{F}_3)$ is the polynomial algebra in one variable $\mathbb{F}_3[\Delta]$ and $\mathcal{F}(1, \mathbb{F}_3)$ is the subspace of basis (Δ^k) where k runs among positive integers not divisible by 3. The set of Galois representations $R(1, \mathbb{F}_3)$ has only one element, $\bar{\rho} = 1 \oplus \omega_3$ where ω_3 is the cyclotomic character modulo 3. Therefore, every nonzero form $f \in M(1, \mathbb{F}_3)$ is a generalized eigenform, and hence pure. Thus the sets $\mathcal{U}_f, \mathcal{N}_f$ are independent of f and are respectively the sets \mathcal{U}, \mathcal{N} of prime numbers ℓ congruent to 1, 2 modulo 3; the invariant $\alpha(f)$ is $1/2$.

The invariant $h(f)$ is more subtle. Recall from Section 3I that $h(f)$ is the largest integer h such that there exist primes ℓ_1, \dots, ℓ_h in \mathcal{N}_f (that is, congruent to 2 mod 3) such that $T_{\ell_1} \cdots T_{\ell_h} f \neq 0$. According to a result of Anna Medvedowski [2015] $h(f)$ is also the largest h such that $T_2^h f \neq 0$. Using this it is easy to compute the value of $h(\Delta^k)$ for small values of k , as shown below (we omit the values of k divisible by 3 since $h(\Delta^{3k}) = h(\Delta^k)$):

f	Δ	Δ^2	Δ^4	Δ^5	Δ^7	Δ^8	Δ^{10}	Δ^{11}	Δ^{13}	Δ^{14}	Δ^{16}	Δ^{17}	Δ^{19}
$h(f)$	0	1	2	3	4	5	4	5	4	5	4	5	6

In general Medvedowski [2015] has shown that $h(\Delta^k) < 4k^{\log 2 / \log 3}$. Numerical experiments suggest that $h(\Delta^k)$ is of the order \sqrt{k} for large k with $3 \nmid k$, so there is perhaps some room to improve this upper bound (note $\log 2 / \log 3 \approx 0.63$).

Calculation of $\pi(\Delta^2, x)$. The invariant $c(f)$ is the most difficult to determine. We shall calculate $c(\Delta^2)$, illustrating the proof of our theorem in this simplest nontrivial case. To ease notation, set $f = \Delta^2$. The Hecke module Af is a two-dimensional vector space generated by $f = \Delta^2$ and Δ , and the Hecke algebra A_f can be identified with the algebra of dual numbers $\mathbb{F}_3[\epsilon]$, where $\epsilon \Delta^2 = \Delta$ and $\epsilon \Delta = 0$. The value

of the operators T_ℓ and ℓS_ℓ in $A_f = \mathbb{F}_3[\epsilon]$ is given by the following table (see [Bellaïche and Khare 2015, §A.3.1]):

$\ell \pmod{9}$	1, 4, 7	2	5	8
T_ℓ	2	ϵ	2ϵ	0
ℓS_ℓ	1	-1	-1	-1

From this, using (3.3), it is not difficult to compute T_{ℓ^n} for any n :

$\ell \pmod{9}$	1, 4, 7			2			5			8			
$n \pmod{6}$	0, 3	1, 4	2, 5	0, 2, 4	1	3	5	0, 2, 4	1	3	5	0, 2, 4	1, 3, 5
T_{ℓ^n}	1	2	0	1	ϵ	2ϵ	0	1	2ϵ	ϵ	0	1	0

We are now ready to follow the proof of Theorem 1. Since $f \in \mathcal{F}(1, \mathbb{F}_3)$ and f is pure, only Section 4A is relevant. As in our analysis there, write $f = \sum_{n \geq 1} a_n q^n$ and, for $a = 1, 2 \pmod{3}$, let $Z(f, a)$ be the set of integers n such that $a_n = a$. The set $Z(f, a)$ is the disjoint union of sets $Z(f, a; f', f'', h)$ as in (7), where f', f'' are in $Af - \{0\}$ and $h \leq h(f) = 1$ is a nonnegative integer. The subsets with $h = 0$ have negligible contribution in view of (8). When $h = 1$, for the set $Z(f, a; f', f'', 1)$ to be nonempty one must have $h(f'') = 1$ and $h(f') = 0$. Since f'' and f' must be the image of f by some Hecke operators, this implies, in view of the table above, that f'' is either $2\Delta^2$ or Δ^2 and that f' is either 2Δ or Δ , so we have 4 sets $Z(f, a; f', f'', 1)$ to consider for each value 1, 2 of a . As explained in Section 4A, to each permissible choice of f', f'' is attached a set $\mathcal{S}_{f, f''}$ of square-full integers, namely the set of square-full m'' such that $T_{m''} f = f''$, and a multifrobenian set of height 1, that is, a frobenian set, $\mathcal{M}_{f', f''}$, which is the set of primes ℓ in \mathcal{N}_f such that $T_\ell f'' = f'$. For every choice of f'', f' , one sees from the table above that $\mathcal{M}_{f', f''}$ is either the set of primes congruent to 2 (mod 9) or to 5 (mod 9), and in any case $\delta(\mathcal{M}_{f', f''}) = 1/6$. The sets $\mathcal{S}_{f, f''}$ may be easily determined using our table above. Thus $\mathcal{S}_{\Delta^2, \Delta^2}$ consists of square-full numbers where primes $\equiv 2 \pmod{3}$ appear in an even exponent, an even number of primes $\equiv 1 \pmod{3}$ appear in exponents that are at least 2 and $\equiv 1$ or 4 (mod 6), and other primes $\equiv 1 \pmod{3}$ appear in exponents that are multiples of 3. The set $\mathcal{S}_{\Delta^2, 2\Delta^2}$ consists of square-full numbers that are divisible by an odd number of primes $\equiv 1 \pmod{3}$ appearing in exponents at least 2 and $\equiv 1$ or 4 (mod 6), other primes $\equiv 1 \pmod{3}$ appearing in exponents that are multiples of 3, and primes $\equiv 2 \pmod{3}$ appearing in even exponents.

According to Theorem 7, for $a = 1$ or 2, $f' = \Delta$ or 2Δ , and $f'' = \Delta^2$ or $2\Delta^2$, one has

$$\begin{aligned} & \{|n < x : n \in Z(f, a; f', f'', 1)\} \\ & \sim \left(\sum_{s \in \mathcal{S}_{f, f''}} \frac{C(\mathcal{U}, s)}{s} \right) \left(\frac{1}{6} \right) \left(\frac{1}{2} \right) \frac{x}{(\log x)^{\frac{1}{2}}} \log \log x, \quad (18) \end{aligned}$$

where

$$C(\mathcal{U}, s) = C(\mathcal{U}) \prod_{\substack{\ell|s \\ \ell \equiv 1 \pmod{3}}} \left(1 + \frac{1}{\ell}\right)^{-1}$$

and

$$\begin{aligned} C(\mathcal{U}) &= \frac{1}{\Gamma(\frac{1}{2})} \prod_{p \equiv 1 \pmod{3}} \left(1 + \frac{1}{p}\right) \left(1 - \frac{1}{p}\right)^{\frac{1}{2}} \prod_{p \not\equiv 1 \pmod{3}} \left(1 - \frac{1}{p}\right)^{\frac{1}{2}} \\ &= \frac{\sqrt[4]{3}}{\pi \sqrt{2}} \prod_{p \equiv 1 \pmod{3}} \left(1 - \frac{1}{p^2}\right)^{\frac{1}{2}} = 0.2913 \dots \end{aligned} \tag{19}$$

In (18), the factor $1/6$ is $\delta(\mathcal{M}_{f''}, f')$ and the factor $1/2$ is $|\Delta|/|\Gamma|$ (and this factor would disappear if we counted cases $a = 1$ and $a = 2$ together).

Adding up all the possibilities, using (7), we finally obtain that

$$\pi(\Delta^2, x) \sim c(\Delta^2) \frac{x}{(\log x)^{\frac{1}{2}}} \log \log x,$$

where

$$c(\Delta^2) = \frac{1}{3} \sum_{s \in \mathcal{S}_{f, f} \cup \mathcal{S}_{f, 2f}} \frac{C(\mathcal{U}, s)}{s} = \frac{C(\mathcal{U})}{3} \prod_{\ell \equiv 1 \pmod{3}} \left(1 - \frac{1}{\ell^3}\right)^{-1} \prod_{\ell \equiv 2 \pmod{3}} \left(1 - \frac{1}{\ell^2}\right)^{-1}.$$

Calculation of $\pi_{\text{sf}}(\Delta^k, x)$ for $k = 1, 2, 4, 5, 7, 10$. In these examples, we describe the calculation of $c_{\text{sf}}(\Delta^k)$, which is simpler than evaluating $c(\Delta^k)$. For $h \geq 0$ an integer, let \mathcal{M}_h be the set of integers that are the product of exactly h distinct primes, all congruent to 2 or 5 modulo 9. This is a multifrobenian set, attached to the cyclotomic extension $\mathbb{Q}(\mu_9)/\mathbb{Q}$ of the Galois group $G = (\mathbb{Z}/9\mathbb{Z})^*$, and one has $\delta(\mathcal{M}_h) = 2^h / (h!6^h) = 1 / (h!3^h)$. One can show that, for $k = 1, 2, 4, 5, 7, 10$ and $h = h(\Delta^k) = 0, 1, 2, 3, 4, 4$ respectively, and for $m' \in \mathcal{M}_h$, one has (with $f = \Delta^k$) that $T_{m'} f \neq 0$, and in fact $T_{m'} f = \Delta$ or $T_{m'} f = 2\Delta$. Also note that for $f' = \Delta$ or $f' = 2\Delta$, one also has $T_m f' = \Delta$ or 2Δ for any square-free m with prime factors in \mathcal{U} , so that $a_m(f') \neq 0$.

Thus, the main contribution to $Z_{\text{sf}}(\Delta^k)$ is the set we call $\mathcal{Z}(\mathcal{U}, \mathcal{M}_h, 1)$, namely the set of all square-free numbers mm' , where m is any product of primes in \mathcal{U} (i.e., congruent to 1 (mod 3)) and $m' \in \mathcal{M}_h$. According to Theorem 6,

$$\pi_{\text{sf}}(\Delta^k, x) \sim \frac{C(\mathcal{U})}{h!3^h} \frac{x}{(\log x)^{1/2}} (\log \log x)^h, \quad k = 1, 2, 4, 5, 7, 10,$$

where $h = h(k) = 0, 1, 2, 3, 4, 4$ respectively and $C(\mathcal{U})$ is the constant appearing in (19).

7B. Example of a nonpure form in the case $N = 1$, $p = 7$. Examples of powers of Δ that are not pure arise (mod 7). There one has $\Delta^2 = f + \Delta$, where $f = \Delta^2 - \Delta$ is an eigenform for all the Hecke operators T_ℓ (ℓ a prime number with $\ell \neq 7$), with eigenvalue $\ell^2 + \ell^3$. The Galois representation $\bar{\rho}_f$ corresponding to this system is $\omega_7^2 \oplus \omega_7^3$ where ω_7 is the cyclotomic character modulo 7. The set $\mathcal{N}_{\bar{\rho}_f}$ is the set of prime numbers ℓ that are congruent to -1 modulo 7, and $\mathcal{U}_{\bar{\rho}_f}$ is the set of prime numbers congruent to $1, 2, 3, 4, 5$ modulo 7. One has $\alpha(f) = \alpha(\bar{\rho}_f) = 1/6$.

The form Δ is also of course an eigenform, with system of eigenvalues $\ell + \ell^4$ for T_ℓ , corresponding to the Galois representation $\bar{\rho}_\Delta = \omega_7 \oplus \omega_7^4$ with $\alpha(\bar{\rho}_\Delta) = 1/2$.

The decomposition $\Delta^2 = f + \Delta$ is thus the canonical decomposition into pure forms, and the pure form Δ can be neglected because $\alpha(\Delta) > \alpha(f)$. One finds

$$\pi_{\text{sf}}(\Delta^2, x) \sim \pi_{\text{sf}}(f, x) \sim C(\mathcal{U}_{\bar{\rho}_f}) \frac{x}{(\log x)^{1/6}}$$

with

$$C(\mathcal{U}_{\bar{\rho}_f}) = \frac{1}{\Gamma(5/6)} \prod_{\ell \equiv 1, 2, 3, 4, 5 \pmod{7}} \left(1 + \frac{1}{\ell}\right) \left(1 - \frac{1}{\ell}\right)^{\frac{5}{6}} \prod_{\ell \equiv -1, 0 \pmod{7}} \left(1 - \frac{1}{\ell}\right)^{\frac{5}{6}}$$

so that

$$\pi_{\text{sf}}(\Delta^2, x) \sim c_{\text{sf}}(\Delta^2) \frac{x}{(\log x)^{1/6}}, \quad c_{\text{sf}}(\Delta^2) = C(\mathcal{U}_{\bar{\rho}_f}) = 0.5976 \dots$$

Acknowledgement

We are grateful to the referee for a very careful reading of the paper.

References

- [Ahlgren 1999] S. Ahlgren, “Non-vanishing of the partition function modulo odd primes l ”, *Mathematika* **46**:1 (1999), 185–192. MR 2001h:11133 Zbl 0993.11053
- [Bellaïche and Khare 2015] J. Bellaïche and C. Khare, “Level 1 Hecke algebras of modular forms modulo p ”, *Compos. Math.* **151**:3 (2015), 397–415. MR 3320566 Zbl 06434557
- [Bellaïche and Nicolas 2015] J. Bellaïche and J.-L. Nicolas, “Parité des coefficients de formes modulaires”, *The Ramanujan Journal* (2015), 1–44.
- [Chen 2012] S.-C. Chen, “Distribution of the coefficients of modular forms and the partition function”, *Arch. Math. (Basel)* **98**:4 (2012), 307–315. MR 2914347 Zbl 1276.11168
- [Chenevier 2014] G. Chenevier, “The p -adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings”, pp. 221–285 in *Automorphic Forms and Galois Representations* (Durham, NC, 2011), vol. 1, edited by F. Diamond et al., London Mathematical Society Lecture Note Series **414**, Cambridge Univ. Press, 2014.
- [Diamond and Im 1995] F. Diamond and J. Im, “Modular forms and modular curves”, pp. 39–133 in *Seminar on Fermat’s Last Theorem* (Toronto, 1993–1994), edited by V. K. Murty, CMS Conf. Proc. **17**, Amer. Math. Soc., Providence, RI, 1995. MR 97g:11044 Zbl 0853.11032
- [Faber 2012] X. Faber, “Finite p -irregular subgroups of $\text{PGL}_2(k)$ ”, preprint, 2012. arXiv 1112.1999v2

- [Ghitza 2006] A. Ghitza, “All Siegel Hecke eigensystems (mod p) are cuspidal”, *Math. Res. Lett.* **13**:5-6 (2006), 813–823. MR 2008a:11053 Zbl 1185.11032
- [Gouvêa 1988] F. Q. Gouvêa, *Arithmetic of p -adic modular forms*, Lecture Notes in Mathematics **1304**, Springer, Berlin, 1988. MR 91e:11056 Zbl 0641.10024
- [Gross 1990] B. H. Gross, “A tameness criterion for Galois representations associated to modular forms (mod p)”, *Duke Math. J.* **61**:2 (1990), 445–517. MR 91i:11060 Zbl 0743.11030
- [Jochnowitz 1982] N. Jochnowitz, “Congruences between systems of eigenvalues of modular forms”, *Trans. Amer. Math. Soc.* **270**:1 (1982), 269–285. MR 83e:10033b Zbl 0536.10022
- [Katz 1973] N. M. Katz, “ p -adic properties of modular schemes and modular forms”, pp. 69–190. Lecture Notes in Mathematics, Vol. 350 in *Modular functions of one variable, III* (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), edited by W. Kuyk and J.-P. Serre, Springer, Berlin, 1973. MR 56 #5434 Zbl 0271.10033
- [Katz 1975] N. M. Katz, “Higher congruences between modular forms”, *Ann. of Math. (2)* **101** (1975), 332–367. MR 54 #5120 Zbl 0356.10020
- [Medvedovki 2015] A. Medvedovki, *Lower bounds on dimensions of mod- p Hecke algebras: the nilpotence method*, Ph.D. thesis, Brandeis University, 2015, <http://people.brandeis.edu/~medved/Data/DissertationMedvedovsky.pdf>.
- [Miyake 2006] T. Miyake, *Modular forms*, 2nd ed., Springer, Berlin, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda. MR 2006g:11084 Zbl 1159.11014
- [Nicolas and Serre 2012a] J.-L. Nicolas and J.-P. Serre, “Formes modulaires modulo 2: l’ordre de nilpotence des opérateurs de Hecke”, *C. R. Math. Acad. Sci. Paris* **350**:7-8 (2012), 343–348. MR 2922080 Zbl 1275.11073
- [Nicolas and Serre 2012b] J.-L. Nicolas and J.-P. Serre, “Formes modulaires modulo 2: structure de l’algèbre de Hecke”, *C. R. Math. Acad. Sci. Paris* **350**:9-10 (2012), 449–454. MR 2929047 Zbl 1275.11074
- [Serre 1973] J.-P. Serre, “Congruences et formes modulaires”, *Séminaire Bourbaki* **14**:416 (1973), 319–338. Zbl 0276.14013
- [Serre 1976] J.-P. Serre, “Divisibilité de certaines fonctions arithmétiques”, *Enseignement Math. (2)* **22**:3-4 (1976), 227–260. MR 55 #7958 Zbl 0355.10021
- [Serre 2012] J.-P. Serre, *Lectures on $N_X(p)$* , Chapman & Hall/CRC Research Notes in Mathematics **11**, CRC Press, Boca Raton, FL, 2012. MR 2920749 Zbl 1238.11001
- [Tenenbaum 1995] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 2nd ed., Cours Spécialisés [Specialized Courses] **1**, Société Mathématique de France, Paris, 1995. MR 97e:11005a Zbl 0880.11001

Communicated by Barry Mazur

Received 2014-10-29

Revised 2015-07-05

Accepted 2015-08-03

jbellaic@brandeis.edu

*Department of Mathematics, Brandeis University,
415 South Street, Waltham, MA 02453, United States*

ksound@math.stanford.edu

*Department of Mathematics, Stanford University, 450 Serra
Mall, Building 380, Stanford, CA 94305-2125, United States*

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
John H. Coates	University of Cambridge, UK	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Anand Pillay	University of Notre Dame, USA
Brian D. Conrad	Stanford University, USA	Victor Reiner	University of Minnesota, USA
Hélène Esnault	Freie Universität Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Andrew Granville	Université de Montréal, Canada	J. Toby Stafford	University of Michigan, USA
Joseph Gubeladze	San Francisco State University, USA	Ravi Vakil	Stanford University, USA
Roger Heath-Brown	Oxford University, UK	Michel van den Bergh	Hasselt University, Belgium
Craig Huneke	University of Virginia, USA	Marie-France Vignéras	Université Paris VII, France
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Kei-Ichi Watanabe	Nihon University, Japan
János Kollár	Princeton University, USA	Efim Zelmanov	University of California, San Diego, USA
Yuri Manin	Northwestern University, USA	Shou-Wu Zhang	Princeton University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne		

PRODUCTION

production@msp.org
Silvio Levy, Scientific Editor


See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2015 is US \$255/year for the electronic version, and \$440/year (+\$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW[®] from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2015 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 9 No. 8 2015

<i>G</i> -valued crystalline representations with minuscule p -adic Hodge type BRANDON LEVIN	1741
Indicators of Tambara–Yamagami categories and Gauss sums TATHAGATA BASAK and RYAN JOHNSON	1793
The number of nonzero coefficients of modular forms (mod p) JOËL BELLAÏCHE and KANNAN SOUNDARARAJAN	1825
Noetherianity for infinite-dimensional toric varieties JAN DRAISMA, ROB EGGERMONT, ROBERT KRONE and ANTON LEYKIN	1857
On differential modules associated to de Rham representations in the imperfect residue field case SHUN OHKUBO	1881



1937-0652(2015)9:8;1-1