COMPOSITIO MATHEMATICA

Random ordering in modulus of consecutive Hecke eigenvalues of primitive forms

Yuri F. Bilu, Jean-Marc Deshouillers, Sanoli Gun and Florian Luca

Compositio Math. **154** (2018), 2441–2461.

doi:10.1112/S0010437X18007455

FOUNDATION COMPOSITIO MATHEMATICA

LONDON MATHEMATICAL SOCIETY
EST. 1865

Compositio Math. 154 (2018) 2441–2461
doi:10.1112/S0010437X18007455

Random ordering in modulus of consecutive Hecke eigenvalues of primitive forms

Yuri F. Bilu, Jean-Marc Deshouillers, Sanoli Gun and Florian Luca

Abstract

Let $\tau(\cdot)$ be the classical Ramanujan τ-function and let k be a positive integer such that $\tau(n) \neq 0$ for $1 \leqslant n \leqslant k/2$. (This is known to be true for $k < 10^{23}$, and, conjecturally, for all k.) Further, let σ be a permutation of the set $\{1, \ldots, k\}$. We show that there exist infinitely many positive integers m such that $|\tau(m + \sigma(1))| < |\tau(m + \sigma(2))| < \cdots < |\tau(m + \sigma(k))|$. We also obtain a similar result for Hecke eigenvalues of primitive forms of square-free level.

1. Introduction

Throughout the article a *primitive form* of weight κ and level N means a holomorphic cusp form of weight κ for $\Gamma_0(N)$ with the trivial character which is also a normalized Hecke eigenform for all Hecke operators as well of all Atkin–Lehner involutions (see [Ono04, p. 29] for more details). Throughout the paper, we will also assume that N is square-free. A *non-CM primitive form* is an abbreviation for 'primitive form without complex multiplication'.

Let f be a primitive form and

$$f(z) := \sum_{n \geqslant 1} a_f(n) q^n, \quad q = e^{2\pi i z}$$

be its Fourier expansion at $i\infty$. In particular, if f is of weight $\kappa = 12$ and level $N = 1$ then

$$f(z) = \Delta(z) := \sum_{n \geqslant 1} \tau(n) q^n = q \prod_{\ell \geqslant 1} (1 - q^\ell)^{24},$$

where $\tau(n)$ is the classical Ramanujan function.

It is well known that the Fourier-coefficients $a_f(n)$ of any such primitive form f are totally real algebraic numbers. There are quite a few results demonstrating 'random' behavior of the signs of $\tau(n)$, or, more generally, the coefficients of a general primitive forms; see, for instance, [GS12, GKR15, KS09, Mat12, MR15] and the references therein. For instance, Matomäki and Radziwiłł [MR15] have shown that the non-zero coefficients of primitive forms for $\Gamma_0(1)$ are positive and negative with the same frequency. They also show that for large enough x, the number of sign changes in the sequence $\{a_f(n)\}_{n \leqslant x}$ is of the order of magnitude

$$\#\{n \leqslant x : a_f(n) \neq 0\} \asymp x \prod_{\substack{p \leqslant x \\ a_f(p) = 0}} \left(1 - \frac{1}{p}\right).$$

Received 16 February 2017, accepted in final form 25 May 2018, published online 18 October 2018.
2010 Mathematics Subject Classification 11F30 (primary), 11F11, 11N36 (secondary).
Keywords: Fourier coefficients of modular forms, sieve, Sato–Tate.

In this paper, we work in a different direction, and study the behavior of absolute values of non-zero coefficients. Classical results of Rankin [Ran39, Ran70]

$$\sum_{n\leqslant x}|\tau(n)|^2 \asymp x^{12} \quad \text{and} \quad \limsup_{n\to\infty}\frac{|\tau(n)|}{n^{11/2}} = +\infty$$

imply that the sequence $|\tau(n)|$ is not ultimately monotonic; in other words, each of the inequalities

$$|\tau(m+1)| < |\tau(m+2)|, \quad |\tau(m+2)| < |\tau(m+1)|$$

holds for infinitely many m. In this article we obtain (as a special case of a more general result) a similar statement for more than two consecutive values of τ.

THEOREM 1.1. *Let k be a positive integer such that*

$$\tau(n) \neq 0 \quad (1 \leqslant n \leqslant k/2). \tag{1.1}$$

Then for every permutation σ of the set $\{1,\ldots,k\}$, there exist infinitely many positive integers m such that

$$0 < |\tau(m+\sigma(1))| < |\tau(m+\sigma(2))| < \cdots < |\tau(m+\sigma(k))|. \tag{1.2}$$

In fact, existence of at least one m satisfying (1.2) implies (1.1) (see Theorem 1.4 below); in other words, (1.1) is a necessary and sufficient condition for (1.2) to happen infinitely often.

It is known [ZY15, Theorem 1.4] that $\tau(n) \neq 0$ when

$$n \leqslant 982\,149\,821\,766\,199\,295\,999 \approx 9 \times 10^{20}.$$

We also refer to [DvHZ13, Corollary 1.2], which claims that $\tau(n) \neq 0$ for all

$$n \leqslant 816\,212\,624\,008\,487\,344\,127\,999 \approx 8 \times 10^{23}.$$

According to a famous conjecture of Lehmer, $\tau(n) \neq 0$ for all n. If this conjecture holds true, then Theorem 1.1 applies to all k.

In this context, one has another famous conjecture known as Maeda's conjecture. Let $T_n(x)$ be the characteristic polynomial of the nth Hecke operator T_n acting on the vector space of cusp forms of weight κ and level 1, denoted $S_\kappa(1)$. It is well known that $T_n(x)$ is a polynomial with integer coefficients. Maeda [HM97] conjectured that for any non-zero natural number n, the polynomial $T_n(x)$ is irreducible over $\mathbb{Q}$ with Galois group $\mathfrak{S}_d$, where d is the dimension of $S_\kappa(1)$ and $\mathfrak{S}_d$ is the symmetric group on d symbols. If the dimension d of $S_\kappa(1)$ is strictly greater than one and Maeda's conjecture is true, then Theorem 1.1 applies to all k. However, Maeda's conjecture does not imply Lehmer's conjecture.

Our principal result is the following general theorem.

THEOREM 1.2. *Let $f_1,\ldots,f_k$ be primitive forms of square-free levels, not necessarily of same weights, and $\nu_1,\ldots,\nu_k$ be distinct positive integers such that*

$$a_{f_i}(\nu_i) \neq 0 \quad (1 \leqslant i \leqslant k).$$

Then there exist infinitely many positive integers m such that

$$0 < |\lambda_{f_1}(m+\nu_1)| < |\lambda_{f_2}(m+\nu_2)| < \cdots < |\lambda_{f_k}(m+\nu_k)|, \tag{1.3}$$

where $\lambda_{f_i}(n) = a_{f_i}(n)/n^{(\kappa_i-1)/2}$ for any positive integer n and $1 \leqslant i \leqslant k$.

In fact, we prove (see Remark 5.8) that for sufficiently large positive number x, there are at least $cx/(\log x)^k$ positive integers $m \leqslant x$ satisfying (1.3). Here $c > 0$ depends on $f_1, \ldots, f_k, \nu_1, \ldots, \nu_k$ and 'sufficiently large' translates as 'exceeding a certain quantity depending on $f_1, \ldots, f_k, \nu_1, \ldots, \nu_k$'.

It is clear from our proof that, when the forms $f_1, \ldots, f_k$ have equal weights, inequality (1.3) holds true with $a_{f_i}(\cdot)$ instead of $\lambda_{f_i}(\cdot)$. An interesting special case occurs when $f_1 = \cdots = f_k = f$.

Theorem 1.3. *Let f be a primitive form of square-free level and $\nu_1, \ldots, \nu_k$ be distinct positive integers such that*

$$a_f(\nu_i) \neq 0 \quad (1 \leqslant i \leqslant k).$$

Then there exist infinitely many positive integers m such that

$$0 < |a_f(m + \nu_1)| < |a_f(m + \nu_2)| < \cdots < |a_f(m + \nu_k)|. \tag{1.4}$$

In particular, if k is a positive integer such that

$$a_f(n) \neq 0 \quad (1 \leqslant n \leqslant k), \tag{1.5}$$

then for every permutation σ of the set $\{1, \ldots, k\}$, there exist infinitely many positive integers m such that

$$0 < |a_f(m + \sigma(1))| < |a_f(m + \sigma(2))| < \cdots < |a_f(m + \sigma(k))|. \tag{1.6}$$

In fact, one can do even better: to give a necessary and sufficient condition for having (1.6) infinitely often.

Theorem 1.4. *Let k be a positive integer. Then for a primitive form f of square-free level the following three conditions are equivalent.*

(A) *We have*

$$a_f(n) \neq 0 \quad (1 \leqslant n \leqslant k/2). \tag{1.7}$$

(B) *For some positive integer ν we have*

$$a_f(\nu + n) \neq 0 \quad (1 \leqslant n \leqslant k). \tag{1.8}$$

(C) *For every permutation σ of the set $\{1, \ldots, k\}$, there exist infinitely many positive integers m such that*

$$0 < |a_f(m + \sigma(1))| < |a_f(m + \sigma(2))| < \cdots < |a_f(m + \sigma(k))|.$$

Theorem 1.1 follows from this theorem if we take $f = \Delta$.

Remark 1.5. Since it is known that there are no primitive forms with complex multiplications for square-free level (see [Rib77, § 3] and [Rib80, Theorem 3.9]), the primitive forms considered by us are necessarily non-CM.

Techniques of the proofs rely on elementary arguments, sieve methods (Brun's sieve, the Bombieri–Vinogradov theorem), and validity of the Sato–Tate conjecture for non-CM forms. Similar results may be expected for Maass forms, but for the time being, we do not even know that $a_{f_i}(\nu_i) \neq 0$ for a positive proportion of ν_i though it is expected to be true for Maass forms of eigenvalue strictly greater that $1/4$. Also the analogs of the Ramanujan–Petersson and the Sato–Tate conjectures are not known to be true.

For our construction of special values of m for which (1.3) and (1.4) holds, we choose by force the small prime factors of the $m+\nu_i$ so that their contribution ensures the wished ordering of the $|\lambda_f(m+\nu_i)|$ or $|a_f(m+\nu_i)|$, with a little margin, and we expect that the larger prime factors will contribute only within the margin. The first step is to eliminate, thanks to the 'fundamental lemma' of the Sieve theory, the midsize primes. Only the large primes remain, which are essentially bounded in number. To keep control of their contribution, we need to avoid the prime powers, which is easily done (§ 3.4) since we have an explicit bound for the sum of the inverse of the squares larger than z. We are happy that Ramanujan's conjecture, proved by Deligne, ensures that the contribution of the large primes is never very large, but we have to take care of those large primes for which $|\lambda_f(p)|$ or $|a_f(p)|$ is small (thanks to our colleagues who worked hard to prove the Sato–Tate conjecture [BGHT11, CHT08, HST10], we know that those primes are not too numerous), but we do not have explicit bounds as we have for the prime powers. This is where we need to trade the sifting level, which can be small for the sieve part, but which has to be large enough to insure that the contribution of the large 'bad' primes is small.

The article is organized as follows. In § 2, we briefly review the properties of the coefficients of primitive forms used in the sequel. In §§ 3 and 4, we obtain two sieving results instrumental for the proof of Theorems 1.2–1.4. Finally, these theorems are proved in §§ 5 and 6, respectively.

1.1 Conventions

Unless the contrary is stated explicitly:

- p (with or without indices) denotes a prime number;
- κ denotes a positive even integer;
- i, j, k, ℓ, m (with or without indices) denote positive integers;
- n (with or without indices) denotes a non-negative integer;
- d (with or without indices) denotes a square-free positive integer;
- ε, δ denote real numbers satisfying $0 < \varepsilon, \delta \leqslant 1/2$;
- x, y, z, t denote real numbers satisfying $x, y, z, t \geqslant 2$.

2. Hecke eigenvalues of primitive forms

In this section, we list some well-known properties of the Hecke eigenvalues of primitive forms which will be used in the proof of Theorems 1.2 and 1.3.

First of all, the Hecke eigenvalues $a_f(n)$ are multiplicative:

$$a_f(mn) = a_f(m)a_f(n) \quad (m, n \geqslant 1, \gcd(m, n) = 1). \tag{2.1}$$

Furthermore, the values of a_f at prime powers satisfy the following recurrence relations

$$\begin{aligned} &a_f(p^{\ell+1}) = a_f(p)^{\ell+1} \quad \text{if } p|N, \\ &a_f(p^{\ell+1}) = a_f(p)a_f(p^\ell) - p^{\kappa-1}a_f(p^{\ell-1}) \quad \text{if } (p, N) = 1 \ (\ell = 1, 2, \ldots), \end{aligned} \tag{2.2}$$

where κ is the weight of f.

Both (2.1) and (2.2) were conjectured by Ramanujan when $f = \Delta$ and proved by Mordell [Mor17]. Proofs can be found in many sources; see, for instance [DS05, Proposition 5.8.5].

A much deeper result is the upper bound

$$|a_f(p)| \leqslant 2p^{(\kappa-1)/2}. \tag{2.3}$$

It was also conjectured by Ramanujan when $f = \Delta$ and proved by Deligne [Del74, Théorème 8.2]. Equivalently, the polynomial $T^2 - a_f(p)T + p^{\kappa-1}$ can not have distinct real roots. Hence we may write the roots as

$$\alpha_p = p^{(\kappa-1)/2} e^{i\theta_p}, \quad \bar{\alpha}_p = p^{(\kappa-1)/2} e^{-i\theta_p}, \tag{2.4}$$

with $\theta_p \in [0, \pi]$. As before, we shall write

$$\lambda_f(n) = a_f(n)/n^{(\kappa-1)/2}$$

for any positive integer n. If $\theta_p \neq 0, \pi$ (that is, $\lambda_f(p) \neq \pm 2$) then

$$\lambda_f(p^\ell) = \frac{\sin(\ell+1)\theta_p}{\sin\theta_p}. \tag{2.5}$$

We may add for completeness that

$$\lambda_f(p^\ell) = \begin{cases} (\ell+1), & \theta_p = 0, \\ (-1)^\ell(\ell+1), & \theta_p = \pi. \end{cases} \tag{2.6}$$

Another very deep result is the *Sato–Tate conjecture*, proved recently by Barnet-Lamb *et al.* [BGHT11, Theorem B] (see also [CHT08, HST10]). A convenient way to express it is to use the notion of *relative density* of a set of primes: we say that a set $\mathcal{P}$ of primes has the relative density $\delta(\mathcal{P})$ (*respectively* the relative upper density $\bar{\delta}(\mathcal{P})$) if

$$\delta(\mathcal{P}) = \lim \frac{\#(\mathcal{P} \cap [1,x])}{\pi(x)} \quad \left(\textit{respectively } \bar{\delta}(\mathcal{P}) = \limsup \frac{\#(\mathcal{P} \cap [1,x])}{\pi(x)} \right), \tag{2.7}$$

as $x \to +\infty$, where $\pi(x)$ denotes the number of primes up to x.

The above-mentioned result states that, for a non-CM primitive form f, the numbers $\lambda_f(p)$ are equi-distributed in the interval $[-2, 2]$ with respect to the Sato–Tate measure $(1/\pi)\sqrt{1 - t^2/4}\, dt$. This means that for $-2 \leqslant a \leqslant b \leqslant 2$, we have

$$\delta(\{p \colon \lambda_f(p) \in [a, b]\}) = \frac{1}{\pi} \int_a^b \sqrt{1 - \frac{t^2}{4}}\, dt. \tag{2.8}$$

An immediate consequence of this and Remark 1.5 is the following statement.

Proposition 2.1. *Let f be a primitive form of square-free level. Then the following holds.*

(A) *The relative density of the set of primes p such that $\lambda_f(p)$ belongs to a given interval of length 2ε does not exceed ε.*

(B) *In particular, the relative density of primes p such that $\lambda_f(p) = 0$ or ± 2 is 0.*

We notice that the formulation (A) is convenient to use for our purpose, but our argument could be adapted to the weaker condition

$$\bar{\delta}(\{p \colon \lambda_f(p) \in [-\varepsilon, +\varepsilon]\}) \to 0 \quad \text{as } \varepsilon \to 0.$$

Part (B) was well known long before the proof of the Sato–Tate conjecture. See [Ser81, § 7.2, Théorème 15] for a much more general and quantitatively stronger result.

Equations (2.5) and (2.6) imply that $\lambda_f(p^\ell) = 0$ for some ℓ and $(p, N) = 1$ if and only if $\theta_p/\pi \in \mathbb{Q} \cap (0, 1)$. In fact, one knows the following result.

PROPOSITION 2.2. *Let f be a primitive form of square-free level. Then for all but finitely many primes p we have either $\lambda_f(p) \in \{0, \pm 2\}$ or $\theta_p/\pi \notin \mathbb{Q}$.*

For the proof, see [MM07, Lemma 2.5] (see also [KRW07, Lemma 2.2]).

One may remark that if f is of weight $\kappa \geqslant 4$ then this holds for all p with $(p, N) = 1$ without exception, see [MM07, Proposition 2.4].

3. Sieving

In this section, we establish a sieving result instrumental for the proof of Theorems 1.2 and 1.3. The integer m in this section is not necessarily positive; it can be any integer: positive, negative or 0. The other conventions made in § 1.1 remain intact.

3.1 The Sieving theorem

Let Σ be a finite set of prime numbers. We call $m \in \mathbb{Z}$:

- Σ-*unit*, if all its prime divisors belong to Σ;
- Σ-*square-free*, if m is a product of a Σ-unit and a square-free integer.

Also, for $z \geqslant 2$ we define

$$P_\Sigma(z) = \prod_{\substack{p<z \\ p \notin \Sigma}} p. \tag{3.1}$$

Now let $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{Z}$ be integers satisfying

$$a_i \neq 0, \quad \gcd(a_i, b_i) = 1 \quad (i = 1, \ldots, k), \tag{3.2}$$

$$a_i b_j - a_j b_i \neq 0 \quad (1 \leqslant i < j \leqslant k). \tag{3.3}$$

We consider linear forms $L_i(n) = a_i n + b_i$, and for $x \geqslant z \geqslant 2$ we set

$$\Omega(x, z) = \{n : 1 \leqslant n \leqslant x, \gcd\big(L_1(n) \cdots L_k(n), P_\Sigma(z)\big) = 1\}. \tag{3.4}$$

Finally, we let

$$\Omega_1(x, z) = \{n \in \Omega(x, z) \colon L_1(n), \ldots, L_k(n) \text{ are } \Sigma\text{-square-free composite numbers}\}. \tag{3.5}$$

The principal result of this section is the following theorem.

THEOREM 3.1. *Assume that Σ contains all the primes $p \leqslant 2k$, all the prime divisors of every a_i, and all the prime divisors of every $a_i b_j - a_j b_i$ with $i \neq j$. In other words, we assume that*

$$(2k)! \prod_{i=1}^{k} a_i \prod_{1 \leqslant i < j \leqslant k} (a_i b_j - a_j b_i) \tag{3.6}$$

is a Σ-unit. Then there exist real numbers $\eta, c_1 \in (0, 1/2]$, depending only on k and on the cardinality[1] *$\#\Sigma$ (but not on Σ itself, neither on the integers a_i and b_i), and $z_1 \geqslant 2$ depending on $a_1, \ldots, a_k, b_1, \ldots, b_k$, such that the following holds. For any x and z, satisfying $x^\eta \geqslant z \geqslant z_1$ we have*

$$\#\Omega_1(x, z) \geqslant c_1 \frac{x}{(\log z)^k}.$$

[1] Indicating dependence on k here is somewhat useless, because our hypothesis implies that k is bounded in terms of $\#\Sigma$.

https://doi.org/10.1112/S0010437X18007455 Published online by Cambridge University Press

The first step in the proof of Theorem 3.1 is to obtain a lower bound for $\#\Omega(x,z)$, i.e. we wish to get a lower bound for the number of integers up to x for which the product $L_1(n)\cdots L_k(n)$ has no prime factor up to x^η except from a finite given set Σ; in other words, we are interested in sieving out the prime factors less than x^η except those from Σ, when η is sufficiently small: the adapted tool for this situation is called the 'fundamental lemma', cf. [FI10, § 6.5], [IK04, § 6.4] or [HR74, § 2.8]. Looking more carefully at [HR74], we see that, with the exception of Σ, Theorem 2.6, p. 85, is very close to what we are looking for. In § 3.3, we shall state and prove the variant of Theorem 2.6 we need. We obtain a lower bound of the order $x(\log z)^{-k}$.

In the second step, we need to exclude the cases when at least one of the quantities $L_i(n)$ is a prime number. Assume for example that $L_k(n)=n$, we see that [HR74, Theorem 2.6′, p. 87], applied to the product $L_1(n)\cdots L_{k-1}(n)$ (with $k-1$ instead of k) is, again with the exception of the primes from Σ, very close to what we are looking for. In § 3.4, we shall state and prove the variant of Theorem 2.6′ we need. We obtain an upper bound of the order $x(\log z)^{-k+1}(\log x)^{-1}$, which is smaller than the lower bound from the first step, as soon as z is sufficiently small a power of x, i.e. as soon as η is small enough.

The last step consists in sieving out the elements of $\Omega(x,z)$ divisible by the square of some large prime; the key ingredient is the convergence of the series of the inverses of the squares. This step is performed in § 3.5.

Finally, in § 3.6 we prove Theorem 3.1.

We start by giving in § 3.2 some definition and evaluation of some arithmetic quantities.

3.2 Some arithmetic preliminaries

In the remaining part of § 3, unless the contrary is explicitly stated, the constants implied by the notation $O(\cdot)$, $\ll$, $\gg$ or[2] $\asymp$, may depend only on k. The same convention applies to the constants implied by the expressions like 'sufficiently large'.

In order to avoid a conflict of notation between [HR74] and the general use, we follow, in §§ 3.2–3.4, the use of [HR74] and denote by $\nu(d)$ the number of distinct prime factors of the integer d.

We keep the notation of § 3.1 and let $\ell\in\{k-1,k\}$,

$$F_\ell(n)=L_1(n)\cdots L_\ell(n). \tag{3.7}$$

Let ρ_ℓ be the multiplicative function supported on the square-free numbers and such that

$$\rho_\ell(p)=\begin{cases}\ell, & p\notin\Sigma,\\ 0, & p\in\Sigma.\end{cases}$$

For $z\geqslant 2$, we let

$$W_\ell(z)=\prod_{p\leqslant z}\left(1-\frac{\rho_\ell(p)}{p}\right)=\prod_{p\mid\mathcal{P}_\Sigma(z)}\left(1-\frac{\ell}{p}\right), \tag{3.8}$$

$$W_\ell^{(*)}(z)=\prod_{p\leqslant z}\left(1-\frac{\rho_\ell(p)}{p-1}\right)=\prod_{p\mid\mathcal{P}_\Sigma(z)}\left(1-\frac{\ell}{p-1}\right), \tag{3.9}$$

with the usual convention that an empty product is equal to 1.

[2] We use $A\asymp B$ as a shortcut for $A\ll B\ll A$.

https://doi.org/10.1112/S0010437X18007455 Published online by Cambridge University Press

Our assumption (3.6) implies that the congruence

$$F_\ell(n) = L_1(n) \cdots L_\ell(n) \equiv 0 \bmod p$$

has exactly $\rho_\ell(p) = \ell$ solutions for any prime p which does not belong to the set Σ; moreover, all those solutions are non-zero. Thus, the congruence

$$F_\ell(n) = L_1(n) \cdots L_\ell(n) \equiv 0 \bmod d \tag{3.10}$$

has exactly $\rho_\ell(d) = \ell^{\nu(d)}$ solutions for any square-free d having no prime divisor from the set Σ; moreover all those solutions are coprime with d. This implies

$$|\#\{n \in [1,x] \colon F_\ell(n) \equiv 0 \bmod d\} - x\rho_\ell(d)/d| \leqslant \rho_\ell(d) = \ell^{\nu(d)}. \tag{3.11}$$

Since all primes $p \leqslant 2k$ belong to Σ, we have, for all primes p, the estimates

$$0 \leqslant \frac{\rho_\ell(p)}{p} \leqslant \frac{\rho_\ell(p)}{p-1} \leqslant \frac{1}{2}. \tag{3.12}$$

We trivially have

$$W_\ell(z) \geqslant \prod_{2k<p\leqslant z} \left(1 - \frac{\ell}{p}\right). \tag{3.13}$$

Using (3.12), we get the upper bound

$$W_\ell^{(*)}(z) \leqslant 2^{\#\Sigma} \prod_{2k<p\leqslant z} \left(1 - \frac{\ell}{p-1}\right). \tag{3.14}$$

We also notice that Mertens' result [HW60, Theorem 429], easily implies that there exists constants $C(\ell)$ and $C^{(*)}(\ell)$ such that

$$\prod_{2k<p\leqslant z} \left(1 - \frac{\ell}{p}\right) \sim C(\ell)(\log z)^{-\ell} \quad \text{and} \quad \prod_{2k<p\leqslant z} \left(1 - \frac{\ell}{p-1}\right) \sim C^{(*)}(\ell)(\log z)^{-\ell}. \tag{3.15}$$

The following is a fairly standard result, a proof of which can be found in [TW14, p. 55].

$$\text{As } x \text{ tends to infinity:} \sum_{n\leqslant x} \ell^{\nu(n)} \sim c_\ell x (\log x)^{\ell-1} \quad \text{for some positive } c_\ell. \tag{3.16}$$

For $d > 0$ and a coprime to d, we denote by $\pi(x,d,a)$ the number of primes up to x which are congruent to a modulo d and we let

$$E(x,d,a) = \pi(x,d,a) - \frac{\operatorname{li} x}{\varphi(d)} \quad \text{and} \quad E(x,d) = \max_{\gcd(a,d)=1} |E(x,d,a)|. \tag{3.17}$$

We shall use the following consequence of [HR74, Lemma 3.5, p. 115], which is itself a consequence of the Bombieri–Vinogradov theorem and the trivial upper bound

$$E(x,d) \leqslant x/d + 1. \tag{3.18}$$

LEMMA 3.2. *Let m be a positive integer. For any positive constant U, there exists a positive constant $C_1 = C_1(m,U)$ such that*

$$\sum_{d<x^{1/2}(\log z)^{-C_1}} \mu^2(d) m^{\nu(d)} E(x,d) = O_{U,m}\left(\frac{x}{(\log z)^U}\right). \tag{3.19}$$

3.3 Sieving away small prime factors

In this section, we prove the following result.

Proposition 3.3. *With the above notation and assumption (3.6), we have for* $2 \leqslant z \leqslant x$

$$\#\Omega(x,z) = xW_k(z)(1+O(E_0(x,z))), \tag{3.20}$$

where

$$E_0(x,z) = \exp(-u(\log u - \log\log u - \log k - 2)) + \frac{1}{\log z}, \tag{3.21}$$

and

$$u = \log x / \log z. \tag{3.22}$$

Proof. We are going to use [HR74, Theorem 2.5′], noticing that in the main relation, $\log x/\alpha$ is to be read $\log(\kappa/\alpha)$. We refer the reader to [HR74] for the statement of Theorem 2.5′, as well as the notation given there. Let us write the dictionary between the notation from [HR74] and our notation:

$$\begin{aligned}
\mathcal{A} &= \{F_k(n)\colon 1 \leqslant n \leqslant x\},\\
\mathfrak{P} &= \{p\colon p \notin \Sigma\} \quad \text{and} \quad \overline{\mathfrak{P}} = \Sigma,\\
\omega(d) &= \rho_k(d),\\
\kappa &= k,\\
X &= x,\\
U &= 1,\\
\alpha &= 1,\\
R_d &= \#\{n \in [1,x]\colon F_k(n) \equiv 0 \bmod d\} - x\rho_k(d)/d.
\end{aligned}$$

Relation (3.12) implies (Ω_1) (p. 29) with $A_1 = 2$.

By the definition of ρ_k, we have for all p: $\rho_k(p) \leqslant k$, which implies Relation (Ω_0) of [HR74, p. 30], and thus (cf. Lemma 2.2, p. 52) Relation $(\Omega_2(\kappa))$ with $A_2 = \kappa$.

Relations (R_0) and $(R_1(\kappa,1))$ (defined in [HR74, p. 64]), with $L = 1$, $A_0' = k$ and $C_0(U) = 2k + U - 1$ come from (3.11) and (3.16).

We notice that $S(\mathcal{A};\mathfrak{P},z)$ is $\#\Omega(x,z)$ and thus [HR74, Theorem 2.5′] implies our Proposition 3.3. □

3.4 Sieving away prime values

In this part, we are interested in evaluating the cardinality of the set

$$\Omega^{(*)}(x,z) = \{n \leqslant x\colon\ \gcd(L_1(n)\cdots L_{k-1}(n), P_\Sigma(z)) = 1, L_k(n) \text{ prime}\}, \tag{3.23}$$

and we shall prove the following

Proposition 3.4. *With the above notation and assumption (3.6), we have for* $2 \leqslant z \leqslant x$

$$\#\Omega^{(*)}(x,z) = \frac{\mathrm{li}(|a_k|x)}{\varphi(|a_k|)} W_{k-1}^{(*)}(z)(1+O(E^{(*)}(x,z))), \tag{3.24}$$

where

$$E^{(*)}(x,z) = \exp(-(u/3)(\log u - \log\log u - \log(k-1) - 3)) + \frac{1}{(\log z)}, \tag{3.25}$$

and

$$u = \log x / \log z. \tag{3.26}$$

https://doi.org/10.1112/S0010437X18007455 Published online by Cambridge University Press

Proof. We first notice that, without loss of generality, changing if needed (a_i, b_i) into $(-a_i, -b_i)$, we can assume that all the a_i are positive: this is what we assume in the proof.

It will be convenient to let $h = k-1$, $F_h(n) = L_1(n) \times \cdots \times L_h(n)$. We are again going to use [HR74, Theorem 2.5′]. Getting a relation $(R_1(\kappa, \alpha))$ will be more challenging, but the Bombieri–Vinogradov inequality in the form (3.19) will be most helpful. As in the previous section, we start with our dictionary:

$$\begin{aligned}
\mathcal{A} &= \{F_h((q-b_k)/a_k)\colon q \text{ prime}, a_k + b_k \leqslant q \leqslant a_k x + b_k, q \equiv b_k \bmod a_k\},\\
\mathfrak{P} &= \{p\colon p \notin \Sigma\} \quad \text{and} \quad \overline{\mathfrak{P}} = \Sigma,\\
\omega(d) &= d\rho_h(d)/\varphi(d),\\
\kappa &= h = k-1,\\
X &= \mathrm{li}(a_k x)/\varphi(a_k),\\
U &= 1,\\
\alpha &= 1/2,\\
R_d &= \#\{a \in \mathcal{A}\colon d \mid a\} - \frac{\omega(d)}{d} X.
\end{aligned}$$

We check the validity of Relations (Ω_0) and $(\Omega_2(\kappa))$ by the same argument as in § 3.3.

We notice that R_d is defined in terms of the cardinality of $\mathcal{A}_d$; it is more convenient for us to consider, for d having no prime divisor from Σ, the set

$$\mathcal{B}_d = \left\{ q \in [a_k + b_k, a_k x + b_k]\colon q \text{ prime}, q \equiv b_k \bmod a_k, d \mid F_h\left(\frac{q-b_k}{a_k}\right)\right\}$$

which has the same cardinality as $\mathcal{A}_d$. By the remark concerning the solutions of (3.10) and the fact that d and a_k are coprime, there exists a set $T_k(d) \subset (\mathbb{Z}/a_k d\mathbb{Z})^*$ with cardinality $\#T_k(d) = h^{\nu(d)}$ such that

$$q \in \mathcal{B}_d \iff q \in [a_k + b_k, a_k x + b_k] \quad \text{and} \quad q \bmod a_k d \in T_k(d).$$

We thus have, for d having no prime factor from Σ

$$\begin{aligned}
\#\mathcal{A}_d = \#\mathcal{B}_d &= \sum_{t \in T_k(d)} (\pi(a_k x, a_k d, t) + O(1))\\
&= h^{\nu(d)} \left(\frac{\mathrm{li}(a_k x)}{\varphi(a_k d)}\right) + O(h^{\nu(d)}(E(a_k x, a_k d) + 1))\\
&= \frac{h^{\nu(d)}}{\varphi(d)} X + O(h^{\nu(d)}(E(a_k x, a_k d) + 1)),
\end{aligned}$$

which implies

$$R_d = O(h^{\nu(d)}(E(a_k x, a_k d) + 1)). \tag{3.27}$$

Relation (R_0) comes from the previous relation, the trivial upper bound $E(a_k x, a_k d) \leqslant x/d + 1$ and the definition of X.

Relation $(R(\kappa, 1/2))$ comes from Lemma 3.2 and relation (3.16).

We can now apply [HR74, Theorem 2.5′] and get Proposition 3.4 with a slightly better constant and $u = \log X/\log z$. It is more convenient for us to state the result in terms of $u = \log x/\log z$. □

3.5 Sieving away non-square-free values

We also want to count n such that $L_i(n)$ is not Σ-square-free. This is relatively easy. Set

$$M = \max\{|a_1|, \dots, |a_k|, |b_1|, \dots, |b_k|\}.$$

Proposition 3.5. *In the set-up of Theorem 3.1, for $x \geqslant z \geqslant 2$ the set $\Omega(x, z)$ has at most*

$$kM\frac{x+1}{z-1} + k\sqrt{Mx+M}$$

elements n such that $L_i(n)$ is not Σ-square-free for some i.

Proof. If $L_i(n)$ is not Σ-square-free for some $n \in \Omega(x, z)$, then $p^2 \mid L_i(n)$ for some $p \geqslant z$. For a fixed p and i, the number of positive integers n with the property $p^2 \mid L_i(n)$ does not exceed $(|a_i|x + |b_i|)/p^2 + 1$. Summing up over all $p \geqslant z$ and $i = 1, \dots, k$, we estimate the total number of $n \in \Omega(x, z)$ such that some $L_i(n)$ is not Σ-square-free as

$$k(Mx + M)\sum_{p \geqslant z}\frac{1}{p^2} + k\pi(\sqrt{Mx+M}).$$

The infinite sum above is bounded by $1/(z-1)$, whence the result. □

3.6 Proof of Theorem 3.1

We are now ready to prove Theorem 3.1.

The reader will easily check that one can find constants c_1, z_1 and η satisfying the properties required in the statement of Theorem 3.1 such that the following inequalities are valid for any real numbers x and z satisfying $x^\eta \geqslant z \geqslant z_1$.

By Proposition 3.3, (3.13) and (3.15), one has

$$\#\Omega(x, z) \geqslant (1/2)xW_k(z) \geqslant (1/4)C(k)x(\log x)^{-k} \geqslant 3c_1x(\log x)^{-k}. \tag{3.28}$$

Let us denote by $\Omega^{\text{prime}}(x, z)$ the set of the elements n in $\Omega(x, z)$ for which one of the values $L_i(n)$ is prime; applying Proposition 3.4 k times, (3.14) and (3.15), we obtain

$$\#\Omega^{\text{prime}}(x, z) \leqslant 2k\,\mathrm{li}\Big(\Big(\max_i |a_i|\Big)x\Big)W_{k-1}^{(*)}(z) \leqslant c_1x(\log x)^{-k}. \tag{3.29}$$

Let us denote by $\Omega^{\text{square}}(x, z)$ the set of the elements n in $\Omega(x, z)$ for which one of the values $L_i(n)$ is not Σ-square-free. Proposition 3.5 tells us that we have

$$\#\Omega^{\text{square}}(x, z) \leqslant kM\frac{x+1}{z-1} + k\sqrt{Mx+M} \leqslant c_1x(\log x)^{-k}. \tag{3.30}$$

We have

$$\#\Omega_1(x, z) \geqslant \#\Omega(x, z) - \#\Omega^{\text{prime}}(x, z) - \#\Omega^{\text{square}}(x, z) \tag{3.31}$$

and Theorem 3.1 comes from (3.31), (3.28), (3.29) and (3.30).

https://doi.org/10.1112/S0010437X18007455 Published online by Cambridge University Press

4. Avoiding prime factors from a sparse set

In this section, we further refine the set $\Omega_1(x,z)$ constructed in Theorem 3.1, showing that it has 'many' elements n such that $L_1(n)\cdots L_k(n)$ has no prime divisors in a 'sufficiently sparse' set of primes. We will have to impose an additional assumption: every prime from Σ divides every a_i. Probably the statement holds true without this assumption, but imposing it will facilitate the proof, and the result we obtain will suffice for us.

Given an infinite set of primes $\mathcal{P}$, let $\pi_{\mathcal{P}}(x) = \#(\mathcal{P}\cap[0,x])$ and $\bar{\delta}(\mathcal{P})$ be the relative upper density as defined in (2.7). Also let $L_1(n),\ldots,L_k(n)$ and the finite set Σ be as in § 3.1.

Theorem 4.1. *Assume the hypothesis of Theorem 3.1. Moreover, assume that*

$$\text{every } a_i \text{ is divisible by every prime from } \Sigma. \tag{4.1}$$

Let η be the number as in Theorem 3.1. Then there exists $\varepsilon\in(0,1/2]$, depending only on k and on $\#\Sigma$, such that the following holds. For any set $\mathcal{P}$ of primes with $\bar{\delta}(\mathcal{P})\leqslant\varepsilon$, there exists $x_0\geqslant 2$ depending on $a_1,\ldots,a_k,b_1,\ldots,b_k$ and on the set $\mathcal{P}$, such that for $x\geqslant x_0$ at least half of the elements n of the set $\Omega_1(x,x^\eta)$ have the property

$$p\nmid L_1(n)\cdots L_k(n)\quad (p\in\mathcal{P}).$$

Remark 4.2. Condition (4.1) implies that $L_i(n)$ cannot have divisors in Σ; in particular, 'Σ-square-free' from Theorem 3.1 can be replaced by 'square-free'.

We start from an individual prime. In the sequel, we write $a=a_k$, $b=b_k$ and $L(n)=L_k(n)=an+b$. We also set $M=\max\{|a|,|b|\}$.

Proposition 4.3. *Assume the hypothesis of Theorem 3.1. Further, assume that*

$$\text{every prime from } \Sigma \text{ divides } a. \tag{4.2}$$

Then there exist real numbers $C_3\geqslant 2$ depending only on k, and $z_3\geqslant 2$ depending on k and M such that the following holds. Let p be a prime number, $p\notin\Sigma$. Then for any x and z satisfying $x\geqslant z\geqslant z_3$, the set $\Omega_1(x,z)$ has at most $C_3\cdot 2^{\#\Sigma}(x/p)(\log z)^{-k}$ elements n such that $p\mid L(n)$.

Proof. In this proof, every constant implied by $O(\cdot)$, $\ll$ etc. depends only on k. We may assume that $L(n)$ is divisible by p for some $n\in\mathbb{Z}$ (otherwise there is nothing to prove). It follows that $p\nmid a$. (Indeed, if $p\mid a$ then $p\nmid b$ because a and b are coprime, and the congruence $an\equiv -b \bmod p$ is impossible.) Hence, there is a unique $u\in\{0,1,\ldots,p-1\}$ such that $u\equiv -b/a \bmod p$.

For $i=1,\ldots,k$, set

$$a_i'=\begin{cases}a_i, & p\mid L_i(u),\\ pa_i, & p\nmid L_i(u),\end{cases}\qquad b_i'=\begin{cases}L_i(u)/p, & p\mid L_i(u),\\ L_i(u), & p\nmid L_i(u),\end{cases}$$

and write

$$L_i'(n')=a_i'n'+b_i'.$$

An immediate verification shows that (3.2), (3.3) and (3.6) remain true with a_i, b_i and Σ replaced by a_i', b_i' and $\Sigma'=\Sigma\cup\{p\}$. Hence, defining, for $x'\geqslant z'\geqslant 2$, the set

$$\Omega'(x',z')=\{0\leqslant n'\leqslant x' : \gcd(L_1'(n')\cdots L_k'(n'),P_{\Sigma'}(z'))=1\},$$

https://doi.org/10.1112/S0010437X18007455 Published online by Cambridge University Press

we may apply Proposition 3.3: there exists z'_0, depending only on k such that, when $x' \geqslant (z')^{50k}$ and $z' \geqslant z'_0$, we have

$$\#\Omega'(x', z') \ll 2^{\#\Sigma'} \frac{x'}{(\log z')^k} \ll 2^{\#\Sigma} \frac{x'}{(\log z')^k}. \tag{4.3}$$

Every n with $p \mid L(n)$ can be written as $u + n'p$ with $n' \in \mathbb{Z}$. If $n \in \Omega(x, z)$, then clearly we have $0 \leqslant n' \leqslant x/p$. Also,

$$L_i(n) = \begin{cases} pL'_i(n'), & p \mid L_i(u), \\ L'_i(n'), & p \nmid L_i(u) \end{cases} \quad (i = 1, \dots, k).$$

It follows that the number of $n \in \Omega(x, z)$ such that $p \mid L(n)$ is bounded by $\#\Omega'(x/p, z)$.

Unfortunately, we cannot apply (4.3) with $x' = x/p$ and $z' = z$, because we do not have $x' \geqslant (z')^{50k}$. This is the main reason why we had to replace $\Omega(x, z)$ by $\Omega_1(x, z)$, because if $n \in \Omega_1(x, z)$ then we can bound x/p from below.

Indeed, let $n \in \Omega_1(x, z)$ be such that $p \mid L(n)$. By the definition of the set $\Omega_1(x, z)$, we know that $L(n)$ is composite and (4.2) implies that $L(n)$ is not divisible by any primes from Σ. Hence $L(n)/p$ must be divisible by some prime $p' \geqslant z$. In particular, $|L(n)/p| \geqslant z$, which implies that $x/p \geqslant z/M - 1$ (recall that $M = \max\{|a|, |b|\}$). Now setting $x' = x/p$ and $z' = (z/M - 1)^{1/50k}$, we obtain

$$\begin{aligned} \#\{n \in \Omega_1(x, z) : p \mid L(n)\} &\leqslant \#\Omega'(x/p, z) \\ &\leqslant \#\Omega'(x', z') \\ &\ll 2^{\#\Sigma} \frac{x'}{(\log z')^k} \\ &\ll 2^{\#\Sigma} \frac{x/p}{(\log(z/M - 1))^k}, \end{aligned} \tag{4.4}$$

provided

$$(z/M - 1)^{1/50k} \geqslant z'_0. \tag{4.5}$$

If we define $z_3 = \max\{M(z'_0)^{50k} + M, 4M^2\}$, then $z \geqslant z_3$ implies both (4.5) and $z/M - 1 \geqslant z^{1/2}$. Hence, the right-hand side of (4.4) is $O(2^{\#\Sigma}(x/p)(\log z)^{-k})$, as wanted. □

We will also need the following easy lemma.

Lemma 4.4. *Let $\mathcal{P}$ be a set of prime numbers, $\varepsilon \in (0, 1/2]$ and $z_0 \geqslant 2$. Assume that for all $t \geqslant z_0$, we have $\pi_{\mathcal{P}}(t) \leqslant \varepsilon\pi(t)$. Then for $x \geqslant z \geqslant z_0$ we have*

$$\sum_{\substack{p \in \mathcal{P} \\ z \leqslant p < x}} \frac{1}{p} \ll \varepsilon \log\left(\frac{\log x}{\log z}\right) + \varepsilon,$$

the implied constant being absolute.

Proof. Using partial summation, we have

$$\sum_{\substack{p \in \mathcal{P} \\ z \leqslant p < x}} \frac{1}{p} = \frac{\pi_{\mathcal{P}}(x^-)}{x} - \frac{\pi_{\mathcal{P}}(z^-)}{z} + \int_z^x \frac{\pi_{\mathcal{P}}(t)}{t^2}\, dt \ll \varepsilon \log\left(\frac{\log x}{\log z}\right) + \varepsilon,$$

as wanted. □

https://doi.org/10.1112/S0010437X18007455 Published online by Cambridge University Press

Proof of Theorem 4.1. Let η, c_1 and z_1 be as in Theorem 3.1. Then for $x \geqslant z_1^{1/\eta}$, we have $\#\Omega_1 \geqslant c_1 x(\log x)^{-k}$, where we denote $\Omega_1 = \Omega_1(x, x^\eta)$.

Now let $\mathcal{P}$ be a set of prime numbers, and let Ω_2 be the subset of Ω_1 consisting of $n \in \Omega_1$ such that some $p \in \mathcal{P}$ divides $L_1(n) \cdots L_k(n)$. Also let z_3 be as in Proposition 4.3. Define $z_2 \geqslant \max\{z_1, z_3\}$ so large that for $t \geqslant z_2$, we have $\pi_{\mathcal{P}}(t) \leqslant 2\bar{\delta}(\mathcal{P})\pi(t)$, and set $x_0 = z_2^{1/\eta}$. Proposition 4.3 and Lemma 4.4 imply that for $x \geqslant x_0$, we have

$$\begin{aligned}\#\Omega_2 &\ll \frac{x}{(\log x)^k} \sum_{\substack{p \in \mathcal{P} \\ x^\eta \leqslant p < x}} \frac{1}{p} \\ &\ll \bar{\delta}(\mathcal{P}) \frac{x}{(\log x)^k} \left(\log \frac{\log x}{\log x^\eta} + 1 \right) \\ &\ll \bar{\delta}(\mathcal{P}) \frac{x}{(\log x)^k},\end{aligned}$$

where the implicit constants depend on k and on $\#\Sigma$.

It follows that there exists $\varepsilon \in (0, 1/2]$, depending on k and on $\#\Sigma$, such that, when $\bar{\delta}(\mathcal{P}) \leqslant \varepsilon$, we have

$$\#\Omega_2 \leqslant \frac{1}{2} c_1 \frac{x}{(\log x)^k} \leqslant \frac{1}{2} \#\Omega_1.$$

This completes the proof of the theorem. □

5. Proof of Theorems 1.2 and 1.3

Throughout the section, we assume that $f_1, \ldots, f_k$ are primitive forms of square-free levels (as defined in the beginning of § 1) of weights $\kappa_1, \ldots, \kappa_k$ respectively. We also fix, once and for all, distinct positive integers $\nu_1, \ldots, \nu_k$ satisfying $a_{f_i}(\nu_i) \neq 0$ for $i = 1, \ldots, k$. We will assume that $k \geqslant 2$ as otherwise we know that any non-zero primitive form has infinitely many non-zero Fourier coefficients (see Proposition 6.1). Set $K = \max\{\nu_1, \ldots, \nu_k\}$.

5.1 An application of the Chinese remainder theorem

Proposition 5.1. *Let $m \geqslant 1$ be such that*

$$m \equiv 0 \bmod (2K)!. \tag{5.1}$$

There exists a positive real number c_0, depending on K and $f_1, \ldots, f_k$, such that for m satisfying (5.1) we have

$$c_0 |\lambda_{f_i}(m_i)| \leqslant |\lambda_{f_i}(m + \nu_i)| \leqslant c_0^{-1} |\lambda_{f_i}(m_i)| \quad (i = 1, \ldots, k), \tag{5.2}$$

and

$$c_0 |\lambda_{f_i}(m_i)| \leqslant \frac{|a_{f_i}(m + \nu_i)|}{m^{(\kappa_i - 1)/2}} \leqslant c_0^{-1} |\lambda_{f_i}(m_i)| \quad (i = 1, \ldots, k), \tag{5.3}$$

where m_i is defined by

$$m + \nu_i = \nu_i m_i \quad (i = 1, \ldots, k). \tag{5.4}$$

Proof. It follows from (5.1) and the definition of K that each m_i is coprime to $(2K)!$. In particular,

$$\gcd(\nu_i, m_i) = 1 \quad (i = 1, \ldots, k). \tag{5.5}$$

Since $a_{f_i}(\nu_i) \neq 0$ for $i = 1, \ldots, k$, we may define

$$c_0 = \min_{1 \leqslant i \leqslant k} \min\left\{|\lambda_{f_i}(\nu_i)|, \frac{1}{2^{(\kappa_i-1)/2}|\lambda_{f_i}(\nu_i)|}\right\}.$$

Hence, by multiplicativity, we have

$$\frac{|a_{f_i}(m+\nu_i)|}{m^{(\kappa_i-1)/2}} \geqslant |\lambda_{f_i}(m+\nu_i)| = |\lambda_{f_i}(\nu_i)||\lambda_{f_i}(m_i)| \geqslant c_0|\lambda_{f_i}(m_i)|$$

and

$$|\lambda_{f_i}(m+\nu_i)| = |\lambda_{f_i}(\nu_i)||\lambda_{f_i}(m_i)| \leqslant c_0^{-1}|\lambda_{f_i}(m_i)|.$$

This completes the proof of (5.2). Since $m \geqslant 2K$, we have

$$(m+\nu_i)^{(\kappa_i-1)/2} \leqslant 2^{(\kappa_i-1)/2} m^{(\kappa_i-1)/2}$$

and then, again by multiplicativity, one has

$$\begin{aligned}\frac{|a_{f_i}(m+\nu_i)|}{m^{(\kappa_i-1)/2}} &\leqslant 2^{(\kappa_i-1)/2}|\lambda_{f_i}(m+\nu_i)| \\ &= 2^{(\kappa_i-1)/2}|\lambda_{f_i}(\nu_i)||\lambda_{f_i}(m_i)| \\ &\leqslant c_0^{-1}|\lambda_{f_i}(m_i)|.\end{aligned}$$

This completes the proof of (5.3). □

5.2 Sieving and the Sato–Tate conjecture

Next we choose primes $p_1 < \cdots < p_k$ with $p_1 > 2K$ such that

$$\lambda_{f_i}(p_i) \neq \pm 2 \quad (i = 1, \ldots, k), \tag{5.6}$$
$$\lambda_{f_i}(p_i^{\ell}) \neq 0 \quad (i = 1, \ldots, k,\ \ell = 1, 2, \ldots). \tag{5.7}$$

Existence of such primes is guaranteed by Propositions 2.1 and 2.2.

Let $\ell_1, \ldots, \ell_k$ be positive integers which will be specified later. We now impose on m, besides (5.1), the conditions

$$m + \nu_i \equiv p_i^{\ell_i} \bmod p_i^{\ell_i+1} \quad (i = 1, \ldots, k). \tag{5.8}$$

Together with (5.1) this puts m into an arithmetic progression modulo A, where

$$A = (2K)! \prod_{i=1}^{k} p_i^{\ell_i+1}. \tag{5.9}$$

Write $m = An + B$, where $B < A$ is the smallest positive integer in this progression. Here, $n \geqslant 0$ is some non-negative integer. Then $m + \nu_i = \nu_i p_i^{\ell_i}(a_i n + b_i)$, where

$$a_i = \frac{A}{\nu_i p_i^{\ell_i}}, \quad b_i = \frac{B + \nu_i}{\nu_i p_i^{\ell_i}} \quad (i = 1, \ldots, k) \tag{5.10}$$

are positive integers.[3] In particular, the numbers m_i defined in (5.4) are given by

$$m_i = p_i^{\ell_i} L_i(n) \quad (i = 1, \ldots, k), \tag{5.11}$$

where $L_i(n) = a_i n + b_i$.

[3] There is no risk of confusing the Hecke eigenvalues $a_{f_i}(n)$ and the integers a_i.

Note that

$$\gcd(A, B+\nu_i) = \nu_i p_i^{\ell_i} \quad (i=1,\ldots,k),$$
$$a_ib_j - a_jb_i = \frac{A}{\nu_i\nu_j p_i^{\ell_i} p_j^{\ell_j}}(\nu_j-\nu_i) \quad (1 \leqslant i,j \leqslant k).$$

In particular, it follows that the integers $a_1,\ldots,a_k,b_1,\ldots,b_k$ defined in (5.10) satisfy (3.2) and (3.3). Moreover, setting

$$\Sigma = \{p \leqslant 2K\} \cup \{p_1,\ldots,p_k\},$$

conditions (3.6) and (4.1) hold true as well, which allows us to apply our sieving Theorems 3.1 and 4.1. Using them and the Sato–Tate conjecture (as stated in Proposition 2.1), we obtain the following.

PROPOSITION 5.2. *There exists a positive number c_1, depending on K and on the forms f_i such that there exist infinitely many positive integers n with the following property:*

$$c_1 \leqslant |\lambda_{f_i}(L_i(n))| \leqslant c_1^{-1} \quad (i=1,\ldots,k). \tag{5.12}$$

Proof. Let η and ε be as in Theorem 3.1 and Theorem 4.1 respectively. Both depend on k and $\#\Sigma$, but since $\#\Sigma = \pi(2K)+k$, this translates into dependence on K.

Now let $\mathcal{P}_\varepsilon$ be the set of prime numbers p such that for some $i \in \{1,\ldots,k\}$ we have $|\lambda_{f_i}(p)| \leqslant \varepsilon/k$. Proposition 2.1 implies that its relative density is at most ε. Now Theorems 3.1 and 4.1 together imply that there exist infinitely many positive integers n with the following properties.

(A) Each $L_i(n)$ is a square-free positive integer.

(B) For $i=1,\ldots,k$, every prime $p \mid L_i(n)$ satisfies $p \geqslant n^\eta$.

(C) For $i=1,\ldots,k$, every prime $p \mid L_i(n)$ satisfies $|\lambda_{f_i}(p)| > \varepsilon/k$.

After discarding finitely many numbers n, item (B) implies that

(B′) for $i=1,\ldots,k$, every prime $p \mid L_i(n)$ satisfies $p \geqslant L_i(n)^{\eta/2}$.

Hence, each $L_i(n)$ has at most $2/\eta$ prime divisors. Write $L_i(n) = q_1\cdots q_s$, where $s \leqslant 2/\eta$ and $q_1,\ldots,q_s$ are distinct prime numbers satisfying

$$\frac{\varepsilon}{k} < |\lambda_{f_i}(q_j)| \leqslant 2 \quad (j=1,\ldots,s).$$

The inequality on the right is by Deligne's bound (2.3). By multiplicativity, we now obtain

$$\left(\frac{\varepsilon}{k}\right)^{2/\eta} \leqslant |\lambda_{f_i}(L_i(n))| \leqslant 2^{2/\eta}.$$

This completes the proof. □

Remark 5.3. Slightly modifying the above argument, one proves the following quantitative result: there exist $c_2 > 0$ (depending on K) and $x_0 \geqslant 2$ (depending on K, on the forms f_i and on our choice of the primes p_i and the exponents ℓ_i) such that for $x \geqslant x_0$ the number of $n \leqslant x$ with the property (5.12) is at least $c_2x(\log x)^{-k}$. The constant c_2 is effective, but x_0 is not, because it depends on a 'quantitative' form of the Sato–Tate conjecture, which is not known to be effective (to the best of our knowledge).

5.3 The exponents ℓ_i

We now fix a small parameter $\delta > 0$ (to be specified later) and define, in terms of this δ, our $\ell_1, \dots, \ell_k$.

Proposition 5.4. *Let δ be a positive real number. Then there exist positive integers $\ell_1, \dots, \ell_k$ such that*

$$|\lambda_{f_1}(p_1^{\ell_1})| < \delta|\lambda_{f_2}(p_2^{\ell_2})| < \cdots < \delta^{k-1}|\lambda_{f_k}(p_k^{\ell_k})|. \tag{5.13}$$

We start with an easy lemma.

Lemma 5.5. *Let f be a primitive form of weight κ, let p be a prime number such that $\lambda_f(p) \neq \pm 2$, and let ε a positive real number. Then there exists a positive integer ℓ such that $|\lambda_f(p^\ell)| < \varepsilon$.*

Proof. We may assume $\theta_p/\pi \notin \mathbb{Q}$ as otherwise there is nothing to prove. Using (2.5), we know that

$$|\lambda_f(p^\ell)| = \frac{|\sin((\ell+1)\theta_p)|}{|\sin\theta_p|}.$$

Since $\theta_p/\pi \notin \mathbb{Q}$, selecting ℓ suitably, we can make $|\sin((\ell+1)\theta_p)|$ as small as we please. □

Corollary 5.6. *Let f, g be primitive forms of weights κ, ρ, respectively, and let p, q be prime numbers. Also let ℓ' be a positive integer and δ be a positive real number. Assume that $\lambda_f(p) \neq \pm 2$ and $a_g(q^{\ell'}) \neq 0$. Then there exists a positive integer ℓ such that*

$$|\lambda_f(p^\ell)| < \delta|\lambda_g(q^{\ell'})|.$$

Proof. Apply Lemma 5.5 with $\varepsilon = \delta|\lambda_g(q^{\ell'})|$. □

Proof of Proposition 5.4. Set $\ell_k = 1$ and afterwards define $\ell_{k-1}, \dots, \ell_1$ iteratively by applying Corollary 5.6 $(k-1)$-times. The hypothesis of Corollary 5.6 is assured because of (5.6) and (5.7). □

Remark 5.7. Using Baker's theory of logarithmic forms, it is possible to prove that one can find suitable $\ell_1, \dots, \ell_k$ effectively bounded in terms of $f_1, \dots, f_k$ and δ. We do not go into details since we do not need this.

5.4 Conclusion

Now we are ready to prove Theorems 1.2 and 1.3. Let c_0 and c_1 be as in Proposition 5.1 and Proposition 5.2 respectively. Set $\delta = (c_0c_1)^2/2$ and define the exponents $\ell_1, \dots, \ell_k$ as in Proposition 5.4. (It is crucial here that c_0 and c_1 depend only on K but not on the exponents ℓ_i.) Now if n is one of the infinitely many positive integers satisfying property (5.12), then in the set-up of Theorem 1.2 the corresponding $m = An + B$ satisfies

$$|\lambda_{f_1}(m+\nu_1)| \leqslant \frac{1}{2}|\lambda_{f_2}(m+\nu_2)| \leqslant \cdots \leqslant \frac{1}{2^{k-1}}|\lambda_{f_k}(m+\nu_k)|,$$

as follows from (5.2), (5.11), (5.12) and (5.13). In the set-up of Theorem 1.3 it satisfies

$$|a_f(m+\nu_1)| \leqslant \frac{1}{2}|a_f(m+\nu_2)| \leqslant \cdots \leqslant \frac{1}{2^{k-1}}|a_f(m+\nu_k)|,$$

as follows from (5.3) (with $f_1 = \cdots = f_k = f$), (5.11)–(5.13). This completes the proof of Theorems 1.2 and 1.3.

Remark 5.8. As Remark 5.3 suggests, we actually obtain the following quantitative results: for sufficiently large x, there is at least $cx(\log x)^{-k}$ positive integers $m \leqslant x$ with the property (1.3) and (1.4); here $c = c(K, f_1, \dots, f_k) > 0$ is effective and 'sufficiently large' is not effective.

https://doi.org/10.1112/S0010437X18007455 Published online by Cambridge University Press

6. Proof of Theorem 1.4

In this section k is a positive integer, and f is a primitive form of square-free level, as defined in the beginning of § 1. We want to show that the three conditions (A), (B) and (C) are equivalent. We will assume that $k \geqslant 2$ as otherwise we know that any non-zero primitive form has infinitely many non-zero Fourier coefficients (see Proposition 6.1). Condition (C) trivially implies (B), and (B) implies (C) by putting

$$\nu_i = \nu + \sigma(i) \quad (1 \leqslant i \leqslant k)$$

in Theorem 1.3.

The implication (B) $\Rightarrow$ (A) is easy. One readily sees that (1.7) is equivalent to the following:

$$a_f(p^\ell) \neq 0 \text{ for every prime } p \text{ and positive } \ell \text{ with } p^\ell \leqslant k/2. \tag{6.1}$$

We will check (6.1); let p and ℓ be such that $p^\ell \leqslant k/2$. Since $k \geqslant 2p^\ell$, the set $\{\nu+1, \ldots, \nu+k\}$ contains at least two consecutive multiples of p^ℓ and so one of them, say $\nu + h$, is divisible by p^ℓ but not by $p^{\ell+1}$. Since a_f is multiplicative and $a_f(\nu+h) \neq 0$, we have $a_f(p^\ell) \neq 0$.

We are left with the implication (A) $\Rightarrow$ (B). We deduce it from Theorems 3.1 and 4.1 with the help of the following lemma.

LEMMA 6.1. *Let f be a primitive form of square-free level N. For every prime number p there exist infinitely many integers ℓ such that*

$$a_f(p^\ell) \neq 0.$$

Proof. If $p|N$, then we know from the Atkin–Lehner theory that

$$a_f(p^\ell) = a_f(p)^\ell \neq 0 \tag{6.2}$$

as N is square-free (see [Ono04, p. 29]). We shall now only consider primes p with $(p, N) = 1$. We shall indeed prove that among two consecutive non-negative integers $(\ell, \ell+1)$, at least one, say ℓ', satisfies $a_f(p^{\ell'}) \neq 0$.

Our claim is true for $\ell = 0$ since $a_f(1) = 1$. Let us assume (induction hypothesis) that it is true for a pair $(\ell, \ell+1)$.

If $a_f(p^{\ell+1}) \neq 0$, then our claim is true for the pair $(\ell+1, \ell+2)$. On the other hand, if $a_f(p^{\ell+1}) = 0$, then $a_f(p^\ell) \neq 0$ by our induction hypothesis, and (2.2) implies that

$$a_f(p^{\ell+2}) = a_f(p)a_f(p^{\ell+1}) - p^{\kappa-1}a_f(p^\ell) = -p^{\kappa-1}a_f(p^\ell) \neq 0.$$

Hence, our claim is again true for the pair $(\ell+1, \ell+2)$. This proves the lemma. □

Alternatively, it is possible to deduce the lemma from equations (2.5), (2.6) and (6.2); we leave the details to the reader.

Proof of the implication (A) $\Rightarrow$ (B). We assume that (6.1) holds and want to find a positive integer ν such that (1.8) holds.

Since (6.1) is the same when $k = 2h$ and $k = 2h+1$, namely $a_f(p^\ell) \neq 0$ for $p^\ell \leqslant h$, it is sufficient to consider the case when k is odd, say $k = 2h+1$.

https://doi.org/10.1112/S0010437X18007455 Published online by Cambridge University Press

We define Σ as the set of all primes $p \leqslant 2k$ and those finitely many primes p for which $a_f(p) \neq 0$ but $a_f(p^\ell) = 0$ for some $\ell > 1$. By Lemma 6.1, to each $p \in \Sigma$ we may associate an integer ℓ_p such that

$$a_f(p^{\ell_p}) \neq 0, \tag{6.3}$$
$$p^{\ell_p} > k. \tag{6.4}$$

By the Chinese remainder theorem, one can find a positive integer r such that

$$r \equiv p^{\ell_p} \bmod p^{\ell_p+1} \quad (p \in \Sigma). \tag{6.5}$$

We will show that there exist infinitely many positive integers m such that

$$a_f(Dm + r + j) \neq 0 \quad (-h \leqslant j \leqslant h), \tag{6.6}$$

where

$$D = \prod_{p\in\Sigma} p^{\ell_p+1}.$$

If m is any such integer, then, setting $\nu = r + Dm - h - 1$, we clearly obtain (1.8).

For $-h \leqslant j \leqslant h$, we introduce the linear forms $L_j(m) = a_j m + b_j$ by

$$Dm + r + j = \gcd(D, r + j)L_j(m) = \gcd(D, r + j)(a_j m + b_j).$$

(There is no risk of confusing the Hecke eigenvalues $a_f(n)$ and the integers a_j.) Let us first check that the k linear forms L_j satisfy the conditions of Theorems 3.1 and 4.1.

- By construction, for every j, we have $a_j \neq 0$ and $\gcd(a_j, b_j) = 1$.
- For $i \neq j$, we have $D(r + j) - D(r + i) = D(j - i) \neq 0$. Since $a_i b_j - a_j b_i$ is a divisor of $D|j - i|$, it is not 0.
- By construction, a_i is a divisor of D which has only prime divisors from Σ.
- Similarly, $a_i b_j - a_j b_i$ is a divisor of $D|j - i|$, where D and $|j - i| \leqslant k$ have only prime divisors from Σ.
- We finally have to verify that every a_j is divisible by every prime in the set Σ. Since $r \equiv p^{\ell_p} \bmod p^{\ell_p+1}$ and $p^{\ell_p} > k > h$, we have $\text{ord}_p(r + j) \leqslant \ell_p$ (where ord_p denotes the p-adic valuation). Now since
$$\text{ord}_p(a_j) = \text{ord}_p(D) - \text{ord}_p(r + j)$$
and $p^{\ell_p+1} \mid D$, we have $\text{ord}_p(a_j) \geqslant 1$.

We can now apply Theorems 3.1 and 4.1, taking for the unwanted set of primes those which are not in Σ and for which $a_f(p) = 0$. Thus, there exist infinitely many positive integers m such that each of the k numbers $L_{-h}(m), \ldots, L_h(m)$ is square-free, not divisible by any prime from Σ nor by any prime p for which $a_f(p) = 0$. It follows that for such m, we have

$$a_f(L_j(m)) \neq 0 \quad (-h \leqslant j \leqslant h).$$

In order to prove that for these m we have (6.6), it is enough to prove that

$$a_f(\gcd(D, r + j)) \neq 0 \quad (-h \leqslant j \leqslant h). \tag{6.7}$$

When $j = 0$, for any p in Σ we have $p^{\ell_p} \parallel r$ so that $p^{\ell_p} \parallel \gcd(D, r)$. Since $a_f(p^{\ell_p}) \neq 0$ by (6.3), we obtain $a_f(\gcd(D, r)) \neq 0$ by multiplicativity.

If $j \neq 0$, then, for $p \in \Sigma$ we have $\text{ord}_p(j) < \ell_p$ because $p^{\ell_p} > k$ by (6.4). Hence $p^\mu \parallel \gcd(D, r + j)$ implies that $p^\mu \parallel j$. It follows that $p^\mu \leqslant h \leqslant k/2$, and our assumption (1.7) implies that $a_f(p^\mu) \neq 0$. By multiplicativity, this proves (6.7) for $j \neq 0$ as well.

The proof of the implication (A) $\Rightarrow$ (B) is now complete, and so is the proof of Theorem 1.4. □

ACKNOWLEDGEMENTS

The authors would like to thank the referee for her/his extremely careful reading and relevant suggestions which improved the exposition of the paper. F.L. worked on this paper during a visit to the Institute of Mathematics of Bordeaux as an ALGANT scholar in July 2011. He was partially supported by the ALGANT, by grant CPRR160325161141 and an A-rated scientist award both from the NRF of South Africa, by grant no. 17-02804S of the Czech Granting Agency and by IRN 'GANDA' (CNRS). Yu.B. was partially supported by the ALGANT, by the Indo-European Action Marie Curie (IRSES moduli) and by IRN 'GANDA' (CNRS). J.-M.D. was partially supported by the CEFIPRA project 5401-A, by the Indo-European Action Marie Curie (IRSES moduli) and by IRN 'GANDA' (CNRS). S.G. was visiting the Institute of Mathematics of Bordeaux as an ALGANT scholar in 2014 when she started working on this project. She acknowledges support by the ALGANT, a SERB grant and the DAE number theory plan project. During the final stage of preparation of this paper Yu.B. and J.-M.D. enjoyed hospitality of the Institute of Mathematical Sciences at Chennai. The authors thank Satadal Ganguly, Florent Jouve and Gérald Tenenbaum for helpful advice.

REFERENCES

BGHT11 T. Barnet-Lamb, D. Geraghty, M. Harris and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy II*, Publ. Res. Inst. Math. Sci. **47** (2011), 29–98.

CHT08 L. Clozel, M. Harris and R. Taylor, *Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations. With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras*, Publ. Math. Inst. Hautes Études Sci. **108** (2008), 1–181.

Del74 P. Deligne, *La conjecture de Weil*, Publ. Math. Inst. Hautes Études Sci. **43** (1974), 273–307.

DvHZ13 M. Derickx, M. van Hoeij and J. Zeng, *Computing Galois representations and equations for modular curves $X_H(\ell)$*, Preprint (2013), arXiv:1312.6819.

DS05 F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228 (Springer, Berlin, 2005).

FI10 J. Friedlander and H. Iwaniec, *Opera de Cribro*, Colloquium Publications, vol. 57 (American Mathematical Society, Providence, RI, 2010).

GS12 A. Ghosh and P. Sarnak, *Real zeros of holomorphic Hecke cusp forms*, J. Eur. Math. Soc. (JEMS) **14** (2012), 465–487.

GKR15 S. Gun, W. Kohnen and P. Rath, *Simultaneous sign change of Fourier-coefficients of two cusp forms*, Arch. Math. (Basel) **105** (2015), 413–424.

HR74 H. Halberstam and H.-E. Richert, *Sieve methods*, LMS Monographs, vol. 4 (Academic Press, London, 1974).

HW60 G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fourth edition (Clarendon Press, Oxford, 1960).

HST10 M. Harris, N. Shepherd-Barron and R. Taylor, *A family of Calabi–Yau varieties and potential automorphy*, Ann. of Math. (2) **171** (2010), 779–813.

HM97 H. Hida and Y. Maeda, *Non-abelian base change for totally real fields*, in *Olga Taussky-Todd: In memoriam*, Special issue of the Pacific Journal of Mathematics (1997), 189–217.

IK04 H. Iwaniec and E. Kowalski, *Analytic number theory*, Colloquium Publications, vol. 53 (American Mathematical Society, Providence, RI, 2004).

KS09 W. Kohnen and J. Sengupta, *Signs of Fourier coefficients of two cusp forms of different weights*, Proc. Amer. Math. Soc. **137** (2009), 3563–3567.

KRW07 E. Kowalski, O. Robert and J. Wu, *Small gaps in coefficients of L-functions and $\mathcal{B}$-free numbers in short intervals*, Rev. Mat. Iberoam. **23** (2007), 281–326.

Mat12 K. Matomäki, *On signs of Fourier coefficients of cusp forms*, Math. Proc. Cambridge Philos. Soc. **152** (2012), 207–222.

MR15 K. Matomäki and M. Radziwiłł, *Sign changes of Hecke eigenvalues*, Geom. Funct. Anal. **25** (2015), 1937–1955.

Mor17 L. J. Mordell, *On Mr. Ramanujan's empirical expansions of modular functions*, Proc. Cambridge Philos. Soc. **19** (1917), 117–124.

MM07 M. Ram Murty and V. Kumar Murty, *Odd values of Fourier coefficients of certain modular forms*, Int. J. Number Theory **3** (2007), 455–470.

Ono04 K. Ono, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, CBMS Regional Conference Series in Mathematics, vol. 102 (American Mathematical Society, Providence, RI, 2004).

Ran39 R. A. Rankin, *Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions. I. The zeros of the function $\sum_{n=1}^{\infty}\tau(n)/n^s$ on the line $\Re s = 13/2$. II. The order of the Fourier coefficients of integral modular forms*, Proc. Cambridge Philos. Soc. **35** (1939), 351–372.

Ran70 R. A. Rankin, *An Ω-result for the coefficients of cusp forms*, Math. Ann. **203** (1970), 239–250.

Rib77 K. A. Ribet, *Galois representations attached to eigenforms with Nebentypus*, in *Modular Functions of One Variable V*, Lecture Notes in Mathematics, vol. 601 (Springer, Berlin, 1977), 17–51.

Rib80 K. A. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. **253** (1980), 43–62.

Ser81 J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. Inst. Hautes Études Sci. **54** (1981), 123–201.

TW14 G. Tenenbaum and J. Wu, *Théorie analytique et probabiliste des nombres, 307 exercices corrigés* (Belin, 2014).

ZY15 J. Zeng and L. Yin, *On the computation of coefficients of modular forms: the reduction modulo p approach*, Math. Comp. **84** (2015), 1469–1488.

Yuri F. Bilu yuri@math.u-bordeaux.fr
Université de Bordeaux and CNRS,
Institut de Mathématiques de Bordeaux UMR 5251,
33405 Talence, France

Jean-Marc Deshouillers jean-marc.deshouillers@math.u-bordeaux.fr
Université de Bordeaux, CNRS and Bordeaux INP,
Institut de Mathématiques de Bordeaux UMR 5251,
F-33405 Talence, France

Sanoli Gun sanoli@imsc.res.in
Institute of Mathematical Sciences, HBNI,
C.I.T. Campus, Taramani, Chennai 600 113, India

Florian Luca florian.luca@wits.ac.za
School of Mathematics, University of the Witwatersrand,
Private Bag X3, Wits 2050, South Africa

and

Department of Mathematics,
Faculty of Sciences, University of Ostrava,
30. dubna 22, 701 03 Ostrava 1, Czech Republic

https://doi.org/10.1112/S0010437X18007455 Published online by Cambridge University Press